REQUEST FOR PROPOSALS (RFP)

State of Ohio, Department of Transportation
Office of Contract Sales, Purchasing Services
Jack Marchbanks, Ph. D., Director

Response Submission Deadline (Bid Opening Date):
February 14, 2023, at 1:00 p.m. eastern time

Submitted by:

Company Name: ________________________________

Federal Tax ID No.: ____________________________

<table>
<thead>
<tr>
<th>Physical/Mailing Address:</th>
<th>Remit to Payment Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street Address:</td>
<td></td>
</tr>
<tr>
<td>P.O. Box:</td>
<td></td>
</tr>
<tr>
<td>City:</td>
<td></td>
</tr>
<tr>
<td>St:</td>
<td></td>
</tr>
<tr>
<td>Zip:</td>
<td></td>
</tr>
</tbody>
</table>

Contact Person and Phone Number:
(associated to answer questions
about your company's bid)

E-Mail Address (required):
(person who filled out bid)

E-Mail Address (required):
(for notification of future bid opportunities)

<table>
<thead>
<tr>
<th>Telephone Number</th>
<th>800 Number</th>
<th>Fax Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Return Properly Marked, Complete Bid Packages To:

contracts.purchasing@dot.ohio.gov - Paper bids will NOT be accepted.

VENDORS MUST SUBMIT ANY QUESTIONS, CLARIFICATIONS, OR INQUIRIES REGARDING THIS PROCUREMENT VIA THE FOLLOWING WEBSITE:
https://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Pages/PurchasePBQ1.aspx
Attachments to be submitted in the emailed bid response:

Completed Front Page (Separate Attachment)
Completed Signature Page (Separate Attachment)
Completed Affirmation and Disclosure form (Separate Attachment)
Completed Excel Pricing Page (Separate Attachment)
Exhibit A - Affirmative Action Affidavit
Exhibit A - Affirmative Action Affidavit
Exhibit B - Non-Collusion Affidavit
Exhibit C - Debarment & Suspension Certification
Exhibit D – Certification of Restrictions on Lobbying
Exhibit E – Signed FTA Clauses
Exhibit F – TCSDS Specifications & Scope of Work
   Appendix A: Price Proposal Form (Excel attachment)
   Appendix B: Compliance Matrix (Excel attachment)
Supplemental A
Supplemental S

Send multiple emails, as needed, to complete your submission to contracts.purchasing@dot.ohio.gov - Paper bids will NOT be accepted.

Zip files CANNOT be sent.
INTRODUCTION

The Ohio Department of Transportation (ODOT) is requesting proposals from qualified firms to provide Trip Coordination Scheduling and Dispatching Software (TCSDS) to the Office of Transit. This software will support ODOT’s Mobility Ohio project. Mobility Ohio is a collaboration between Ohio’s state agencies that fund community and human service transportation (HST) and is implementing a pilot Regional Transportation Resource Center (RTRC), a one-stop hub where clients and customers can conveniently schedule trips by phone, online or through a smartphone app for multiple trip purposes.

As the pilot region’s administrator for community transportation, the RTRC will establish contracts with qualified for-profit, non-profit, and public transportation providers and ensure compliance with consistent, updated safety and quality standards that meet or exceed the requirements of the individual HST funder agencies and federal transportation regulations. The RTRC will receive transportation funding from state human service agencies (e.g., Job and Family Services, Department of Developmental Disabilities, etc.) The RTRC will also serve as the hub for mobility management activities throughout the four-county pilot area. The RTRC will focus on finding solutions to unique and unmet community transportation needs in the community through travel training, planning and education. The RTRC’s mobility management section will coordinate community outreach and ensure the ongoing implementation of goals and updates to the Region 9 Regional Public Transit Human Services Coordinated Transportation Plan. Clients, customers, and employers with unique transportation needs will have the opportunity to connect with a county mobility manager for assistance.

The ODOT Office of Transit operates Federal and State funded programs designed to assist Ohio’s public transportation service providers and human service transportation providers to address complex administrative and operating issues and comply with a myriad of Federal and State program rules, regulations, and requirements.

SCOPE OF SERVICES

Please refer to Exhibit F for the entire specifications document.

As eligible travelers request trips, their trip requests go to the Regional Transportation Resource Center (RTRC) which contains the software being procured and described in these specifications. The RTRC assigns each trip to an appropriate transportation provider based on several factors which will be described in Section 6 of the specifications. The specification shows three types of transportation providers (TPs), but there is another way to categorize the providers that we will use in this specification:

• **Open-Door TP**: TP that accepts any client referred to them through one or more funding programs; and
• **Closed-Door TP**: TP that only transports their own clients.

Please note that a TP can be both open-door and closed-door since they could have specific vehicles or vehicle-hours in each category. Further, please note that a TP can be a taxi company.

Overall, these specifications identify functional requirements for the RTRC to perform the following:

• Provide an interface/portal for the five groups of software users - the RTRC, TPs, facilities (e.g., hospital, doctor’s office), funding agencies and trip-making customers/clients - to exchange data and information in order to describe and utilize specific parameters for trip booking, offering, scheduling, matching and assignment, and invoicing and reporting;
• Provide real-time and optimized trip scheduling based on trip requests, trip offering and acceptance, and other parameters such as vehicle and driver characteristics;
• Provide a mechanism for TPs to bill/invoice the RTRC;
• Provide a mechanism for funding agencies to enter/update client eligibility;
• Provide on-board driver terminals (e.g., tablets) for communication of manifests, messaging between drivers and dispatchers, and trip monitoring; and
• Assign trips to providers whose drivers and vehicles meet safety and quality standards specific to a client’s needs.

Potential future requirements include but are not limited to the following:

• Provide the ability to interface with other TCSDS systems that build client profiles (e.g., hospital systems, healthcare facilities, social service agencies. For example, if a hospital initiates a ride request for a discharged patient, the patient’s information (name, address, contact information, etc.) shall be imported into the RTRC TCSDS software automatically;
• Provide the ability to interface with a statewide registry of the eligibility of TPs, drivers, and vehicles to operate human service transportation for various funding programs; and
• Provide the ability to create and use a universal regional pass. For example, the TCSDS software could include an electronic fare payment subsystem that could be used by the transit systems in the pilot region (see below for an explanation of the pilot region).

Table 2 shows the overall requirements that must be met by the proposed trip coordination, scheduling and dispatching (TCSDS) software. Detailed requirements for each function can be found in Section 6 of the specifications, Exhibit F.

### Table 1. Overall TCSDS Software Requirements

<table>
<thead>
<tr>
<th>TPs/ Vehicles</th>
<th>Open-Door TPs/RTRC Dedicated Vehicles*</th>
<th>Open-Door TPs/Non-Dedicated Vehicles**</th>
<th>Closed-Door TPs</th>
</tr>
</thead>
</table>
| Interaction between RTRC and TP | TPs’ vehicles are listed on the RTRC daily schedule by parameters:  
  a. Vehicle tier  
  b. Driver tier  
  c. Hours in service  
  d. Service area/zones | 1. The RTRC will offer the trip to one or more providers depending on certain criteria  
  2. TPs accept trips that they are eligible to provide  
  NOTE: Trips need to match up with driver/vehicle tiers | 1. The RTRC assigns trips  
  2. TPs invoice the RTRC for the service they provide  
  3. TPs submit service data reports to the RTRC |
| Trip Scheduling Process | 1. Client/Client Representative requests trip from the RTRC  
  2. The RTRC schedules client with a TP on the appropriate driver and vehicle tier  
  NOTE: Schedules are optimized so TPs may not know the exact schedule until the day before or the day of the trip. Schedule optimization is | 1. Client/Client Representative requests trip from the RTRC  
  2. The RTRC will offer the trip to one or more providers depending on certain criteria  
  3. TP schedules the trip on a non-dedicated vehicle  
  NOTE: Schedules are optimized in real-time so trips may disappear/reappear throughout the scheduling process.  
  4. After trips are accepted, the RTRC can view vehicles on the daily schedule but the non-RTRC activities of the vehicle are not visible. | 1. TPs communicate trip schedules to the RTRC  
  2. The RTRC authorizes funding for the scheduled trips |
conducted in real-time so that keeping dedicated vehicles full is a priority.

<table>
<thead>
<tr>
<th>TP Technology Requirements</th>
<th>Required: Scheduling and dispatching software with ongoing real-time connection to the RTRC On-board driver terminals (e.g., tablets)</th>
<th>Required: Scheduling and dispatching software with ongoing real-time connection to the RTRC On-board driver terminals (e.g., tablets)</th>
<th>Required: A closed-door provider can use a paper-based scheduling system if necessary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired but not required: Pre-trip/post-trip inspection module on driver terminals (for enforcement of that standard)</td>
<td>Desired but not required: Ability to make non-RTRC activities not available to any software users Pre-trip/post-trip inspection module on driver terminals (e.g., tablets)</td>
<td>Desired but not required: Ability to use RTRC web-based billing and reporting portal On-board driver terminals (e.g., tablets) Pre-trip/post-trip inspection module on driver terminals (e.g., tablets)</td>
<td></td>
</tr>
</tbody>
</table>

*Some providers will choose to allow the RTRC to schedule trips directly onto their vehicle schedules. In this scenario, the provider would “turn over” a route (e.g., Vehicle 1 from 9a-5p) to the RTRC to directly schedule trips on the route.

**Providers who contract with the RTRC will receive trip requests from the RTRC, and decide whether or not to schedule the trips, then inform the RTRC of the trip’s status (accepted or declined). In this scenario, the vehicles are “non-dedicated”.

Based on the specification, the successful vendor must complete the Price Proposal Form in Exhibit F, Appendix A & B: ‘Exhibit F_Appendix A & B – TCSDS Compliance Matrix and Price Proposal Form’. Both Appendix A and B are located within the same excel spreadsheet.

Additionally, proposers must submit completed forms ‘Supplemental A’ and ‘Supplemental S’.

Firms will be evaluated on completeness of submission, knowledge, skills, and abilities to produce TCSDS software that meets the required specifications and responds to ODOT’s needs within a budget that efficiently and effectively contains costs.

**PROPOSAL RESPONSE FORMAT**

I. **Description of Proposer**

Proposers must identify themselves any partner firms or subcontractors in accordance with the following document:
- Name:
- Address:
- Telephone:
- Contact Person:
- Contact Person Email Address:
- Contact Person Phone Number:
- Areas of Expertise for this Response:
  - Major Clients Served (particularly identify any State ODOTs for whom contract services were provided):
  - Is this firm a certified DBE firm in Ohio:
II. Understanding of the Scope of Work

Proposers must complete the proposal and address their qualifications for completing the Scope of Services. An appropriate response to this section will include a completed description of areas in which the proposer’s firm or a firm in the proposer’s consulting team has expertise. Please include a listing of the location of past work performed in each area, names of specific employees proposed to perform work in the identified area, and an indication of the firm’s and employee’s availability to perform work on this contract. If copies of past individual studies are needed, they will be requested as the respective submissions are reviewed. Please do not include them in your proposal. Please note in addressing this element, the contract to be awarded comprise a major level of work with the potential for many hundreds of hours of effort. Include the response to this section as the Work Plan.

III. Management and Organization Support

Submit no more than ten (10) resumes of individuals who will be assigned to the proposed contract, including the project manager. List each individual’s qualifications, familiarity with and understanding of FTA and ODOT grant programs, policies and procedures, and previous experience on similar projects. This applies to the proposing firm and to any firms participating in the team or subcontractors. Include a table of organization identifying participating personnel. Include the response to this section as the Staff Plan.

IV. Cost Containment/DBE Requirements

Cost containment is an important factor in determining how many tasks can be performed under the contract. Under this section, please identify measures to be taken to contain costs. A template Price Proposal Form has been provided for this RFP and the proposer must use this document to develop its price proposal.

Areas to be addressed include direct expenses, overhead expenses, and travel expenses.

This contract makes up ODOT’s primary Disadvantaged Business Enterprise effort for the Office of Transit each year. DBE contractors/subcontractors must be identified in this section with a description of how DBE involvement in a task will be determined. The DBE contractors/subcontractors must perform work meaningful to the contract so peripheral efforts should not be included. Failure to follow through and use the DBE contractors/subcontractors following a contract award will provide cause to exclude a firm from future considerations for this contract.

The selected vendor shall deliver a monthly invoice to ODOT staff at least fifteen (15) calendar days after the last day in the previous month. For example, work performed in the month of July shall be invoiced to ODOT by August 15th.

Include the response to this section as the Cost Proposal.

V. Forms, Certifications and Assurances

All proposers must complete, sign and submit the following enclosed exhibits with their proposal:

- Completed Front Page
- Completed Signature Page
- Completed Affirmation and Disclosure form
- Exhibit A - Affirmative Action Affidavit
- Exhibit A - Affirmative Action Affidavit
- Exhibit B - Non-Collusion Affidavit
Exhibit C - Debarment & Suspension Certification
Exhibit D – Certification of Restrictions on Lobbying
Exhibit E – Signed FTA Clauses
Exhibit F – TCSDS Specifications & Scope of Work
  o Appendix A: Price Proposal Form (Excel attachment)
  o Appendix B: Compliance Matrix (Excel attachment)
Supplemental A
Supplemental S

PROPOSER INSTRUCTIONS

I. Proposal Due Date

i. Delivery of Documents

Emailed submissions for this Request for Proposal will be received until 1:00PM eastern time on January 24, 2023, to the following email address:

contracts.purchasing@dot.ohio.gov

No proposals will be accepted after the date and time specified on this page. No hardcopy proposals will be accepted. ODOT reserves the right to reject any and all proposals. Timely receipt of proposals will be determined by the date and time the emailed proposal is received by the Office of Contracts. Receipt of proposals by any other mechanism other than email delivery to the Office of Contracts shall not be considered timely.

All materials submitted in accordance with this solicitation become the property of the State of Ohio and shall not be returned. All materials submitted in accordance with this solicitation shall remain confidential until Successful Proposer(s) are selected after Round 2 at which time all submitted information becomes part of the public record.

ii. Inquires

Pre-proposal questions must be received no later than the close of business the Thursday prior to the scheduled opening date. An addendum being issued is dependent upon the information received and the impact on the competitive bidding process. All pre-proposal inquiries must have the following: Name of the Sender, Contractor or Company Name, Phone Number, Project Number, Letting Date, a detailed description of the question.

Proposers are NOT to contact any other ODOT office, including District offices, for responses to pre-bid questions.

Department responses will be posted to the following website:

http://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Purchase/PBQ-Answers.doc

Proposal Inquiries may be submitted at this link:

https://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Pages/PurchasePBQ1.aspx
Based upon the content of any received questions/clarifications, proposal requirements may, solely at the discretion of ODOT, be modified, changed or deleted. Any such changes to this RFP will be communicated by addendum and published to the ODOT website at the following URL:

http://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Lists/PurchaseUpcomingITBs/RFP.aspx

II. Commitment to Perform Proposal Services

The proposal must be signed by a duly authorized official of the proposer’s firm, or if a joint venture, by an official from each participating firm.

III. Contract Type

ODOT will award a cost reimbursement contract. ODOT and the successful proposer(s) will negotiate the costs. However, under no circumstance will the unit costs for direct labor, the percent of allowances for overhead and general administration, or the profit exceed the amounts or rates agreed upon prior to entering the contract.

IV. Travel

While not requested as a part of the information submitted, all travel costs are limited by the rates allowed under the applicable ODOT travel directives in place at the time travel is undertaken. The Office of Budget and Management (OBM) sets the mileage reimbursement rate for contractors with state agencies to utilize at the following location: https://obm.ohio.gov/wps/portal/gov/obm/areas-of-interest/agency-overview/obm-travel-rule/obm-travel-rule. This contract will utilize the rate set by OBM as amended quarterly throughout the state fiscal year.

V. Contract Award

Any proposed contract negotiated between ODOT and the successful proposer as a result of this RFP is subject to approval of the ODOT Governance Board. Without ODOT Governance Board approval, the contract will be invalid and unenforceable.

PROPOSAL TERMS AND CONDITIONS

I. Reserved Rights

During the solicitation process, ODOT reserves the following rights:

- To reject any or all proposals, to postpone contractor selection and to resolicit or cancel this procurement if deemed to be in the best interest of the State of Ohio.
- To request additional information from any and all proposers.
- To subject the execution of any contract or task order to the availability of funds and negotiation of agreeable terms with the successful proposer.
- To enter into a contract with any proposer based upon the proposer’s initial offer.
- To waive liability for reimbursement of any costs incurred by proposers responding to this RFP.

II. Rejection of Proposals

ODOT may reject any proposal for the following reasons:
Proposer fails to sign the required forms, certifications, and assurances.
Proposer includes exceptions to the services described under Scope of Services.
Proposal exceeds the fifteen (15) page limit, excluding resumes and required forms and certifications.
Proposal is received after the deadline.
Proposer provides less than sixty (60) days for acceptance.

REQUIRED CONTRACT CLAUSES

Any contract awarded as a result of this solicitation will incorporate the clauses of the standard ODOT contract as well as specific clauses required by FTA. The required FTA clauses and certifications (Exhibit A through Exhibit E) are included. If selected, the proposer must execute the contract and each of the appropriate exhibits prior to ODOT’s execution.

EVALUATION AND SELECTION PROCESS

I. Criteria for Scoring of Technical Proposal

Qualifying technical proposals will be collectively scored by a Proposal Review Team (PRT) appointed by ODOT. For each of the evaluation criteria given in the following score sheet, reviewers will collectively judge whether the technical proposal exceeds, meets, partially meets or does not meet the requirements expressed in the RFP, and assign the appropriate point value, as follows:

<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Does Not Meet Requirement</td>
</tr>
<tr>
<td>6</td>
<td>Partially Meets Requirement</td>
</tr>
<tr>
<td>8</td>
<td>Meets Requirement</td>
</tr>
<tr>
<td>10</td>
<td>Exceeds Requirement</td>
</tr>
</tbody>
</table>

Technical Performance Scoring Definitions:

“Does Not Meet Requirement”- A particular RFP requirement was not addressed in the vendor’s proposal, **Score: 0**

“Partially Meets Requirement”-Vendor proposal demonstrates some attempt at meeting a particular RFP requirement, but that attempt falls below acceptable level, **Score: 6**

“Meets Requirement”-Vendor proposal fulfills a particular RFP requirement in all material respects, potentially with only minor, non-substantial deviation, **Score: 8**

“Exceeds Requirement”-Vendor proposal fulfills a particular RFP requirement in all material respects, and offers some additional level of quality in excess of ODOT expectations, **Score: 10**

A technical proposal’s total PHASE II score will be the sum of the point value for all the evaluation criteria. The review team will collectively score each individual qualifying proposal. Technical proposals which do not meet or exceed a total score of at least **307** points (a score which represents that the selected vendor has the capability to successfully perform the project/program services) out of a maximum of **400** points, will be disqualified from further consideration, and its cost proposal will neither be opened nor considered. Only those vendors whose Technical Proposals meet or exceed the minimum required technical points will advance to PHASE III of the technical proposal score sheet.

II. Scoring Breakdown Table

<table>
<thead>
<tr>
<th>ITEM #</th>
<th>EVALUATION CRITERIA</th>
<th>Weight</th>
<th>Doesn’t Meet 0</th>
<th>Partial Meets 6</th>
<th>Meet 8</th>
<th>Exceed 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORK REQUIREMENTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VENDOR QUALIFICATIONS AND EXPERIENCE

<table>
<thead>
<tr>
<th></th>
<th>Prior experience with trip coordination scheduling dispatching software programs, with emphasis on expertise in the creation and management of similar software systems</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Does the vendors proposal clearly express an understanding of the work to be completed.</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Responsiveness to the Scope of Work as identified in Exhibit F</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Clarity of proposal and work</td>
<td>4</td>
</tr>
</tbody>
</table>

STAFFING PLAN

<table>
<thead>
<tr>
<th></th>
<th>Qualifications of personnel – (education, experience, and training)</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Resumes including identification of Project Manager</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>Access of respondent’s resources and personnel too DOT/local public entities.</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>Availability and responsiveness of proposer’s resources and personnel.</td>
<td>3</td>
</tr>
</tbody>
</table>

PROPOSED WORK PLAN

<table>
<thead>
<tr>
<th></th>
<th>The vendor has demonstrated an understanding of the proposal.</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>The vendor has provided a clear and detailed response in terms of approach, deliverables, and schedule that is broken down by task.</td>
<td>4</td>
</tr>
</tbody>
</table>

Based upon the Grand Total Technical Score earned, does the vendor’s proposal meet or exceed the minimum Technical score of 307 points?

Yes______ No______

(If “No” vendor’s Cost Proposal will NOT be opened)

III. Cost Proposal Points

ODOT will use the information Offeror gives on the Cost Summary Form to calculate Cost Proposal Points. ODOT will calculate the Offeror’s Cost Proposal points after the Offeror’s total technical points are determined, using the following method:

Cost points = (lowest Offeror’s cost/Offeror’s cost) x Maximum Allowable Cost Points as indicated in the “Scoring Breakdown” table. The value is provided in the Scoring Breakdown table. “Cost” = Total identified in the Cost Summary section of Offeror’s Proposal. In this method, the lowest cost proposed will receive the maximum allowable points. Total Cost points will be 150.

The number of points assigned to the cost evaluation will be prorated, with the lowest accepted Cost Proposal given the maximum number of points possible for this criterion. Other acceptable Cost Proposals will be scored as the ratio of the lowest Cost Proposal to the Proposal being scored, multiplied by the maximum number of points possible for this criterion.

An example for calculating cost points, where Maximum Allowable Cost Points Value = 60 points, is the scenario where Offeror X has proposed a cost of $100.00. Offeror Y has proposed a cost of
$110.00 and Offeror Z has proposed a cost of $120.00. Offeror X, having the lowest cost, would get the maximum 60 cost points. Offeror Y’s cost points would be calculated as $100.00 (Offeror X’s cost) divided by $110.00 (Offeror Y’s cost) equals 0.909 times 60 maximum points, or a total of 54.5 points. Offeror Z’s cost points would be calculated as $100.00 (Offeror X’s cost) divided by $120.00 (Offeror Z’s cost) equals 0.833 times 60 maximum points, or a total of 50 points.

Cost Score: ______________

FINAL STAGES OF EVALUATION The Offeror with the highest point total from all phases of the evaluation (Technical Points + Cost Points) will be recommended for the next phase of the evaluation.

Technical Score: __________ + Cost Score: __________ = Total Score: ______________

If ODOT finds that one or more Proposals should be given further consideration, ODOT may select one or more of the highest-ranking Proposals to move to the next phase. ODOT may alternatively choose to bypass any or all subsequent phases and make an award based solely on the Proposal evaluation phase.

IV. Selection Process

The successful proposer will be selected by ODOT staff. ODOT staff will review and score all eligible proposals. Proposers may be contacted to conduct an interview. An interview allows ODOT staff to ask questions about the respective proposals and provide an opportunity for proposers to discuss issues relative to their proposals.

Following this selection process, ODOT staff will recommend a proposer for the TCSDS software to ODOT’s Governance Board. Upon approval from the Governance Board, ODOT staff will contact the successful proposer to execute the contract.

VI. RFP Proposer’s Checklist

The checklist below is provided for proposers to ensure all required elements are included in a proposal. In order to be deemed responsive to the RFP by ODOT, all elements must be met.

| ☐ | Deadline | Submitted electronic proposal on or before January 24, 2023 @ 1 P.M. EDT |
| ☐ | Work Plan | Proposer’s experience, understanding of the work, and quality of response regarding the Scope of Work |
| ☐ | Staff Plan | Qualifications of Proposer’s firm or team of firms including resumes |
| ☐ | Price Proposal | Price proposal as a separate document from the rest of the proposal titled as TCSDS_Compliance Matrix_and_Cost-Proposal_Name of Proposer in the format provided |
| ☐ | Compliance Matrix | Compliance matrix as a separate document from the rest of the proposal titled as TCSDS_Compliance Matrix_and_Cost-Proposal_Name of proposer in the format provided |
| ☐ | Required Forms | Completed and signed forms, certifications, and assurances identified in Exhibits A, B, C, D, E, and F Supplemental Forms A and S |
EXHIBIT A

AFFIRMATIVE ACTION AFFIDAVIT
(to be completed by firms with less than 50 employees)

(STATE OF )
(COUNTY OF )

I, ________________, of the ________________, of _____________________
in the County of ____________________, State of _____________________, of full age, being
duly sworn according to law on my oath depose and state that:

1. I am ____________________, of the firm of ____________________, a bidder making a proposal inclusive upon the above-named project.

2. ________________, does not have 50 employees or more inclusive of all officers and employees of every type.

3. I am familiar with the affirmative action requirements of O.R.C. 125.11.1 and rules and regulations issued by the Ohio Department of Administrative Services pursuant thereto.

4. ________________ has complied with all affirmative action requirements of the State of Ohio, including those required by the O.R.C. 125.11.1 and the rules and regulations issued by the Ohio Department of Administrative Services thereto.

5. I am aware that if ________________ does not comply with O.R.C. 125.11.1 and rules and regulations issued pursuant thereto, that no monies will be paid by ODOT until an affirmative action plan is approved. I understand that the contract may be terminated and ________________ may be debarred from all public contracts for a period up to five (5) years for violation of said provisions.

6. In the event my workforce increases to 50 employees, I must contact the Ohio Affirmative Action office and complete an Employee Information Report.

____________________________
Signature of Authorized Official   Title
EXHIBIT B

NON-COLLUSION AFFIDAVIT

(State of       )
(County of     )

I, ___________________________________ of the __________________ of ____________________________

in the County of ______________________, State of ____________________________, of full age,
being duly sworn according to law on my oath depose and state that:

I am ______________________ of the firm of

_____________________________________, a bidder making a proposal inclusive upon the above named project,
and that I executed the said proposal with full authority to do so: that said bidder has not, directly or
indirectly, entered into any agreement, participated in any collusion, or otherwise taken any action in
restraint of free, competitive bidding in connection with the above named project; and that all statements
contained in said proposal and in this affidavit are true and correct, and made with full knowledge that
ODOT relies upon the truth of the statements contained in said proposal and in the statements contained
in this affidavit in awarding the contract for the said project.

I further warrant that no person or selling agency has been employed or retained to solicit or secure such
contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee,
except bona fide employees or bona fide established commercial or selling agencies

maintained by _________________________________.

(Name of Contractor)

________________________________________
Signature of Authorized Official               Title
EXHIBIT C
CERTIFICATION REGARDING DEBARMENT, SUSPENSION, PROPOSED DEBARMENT, AND OTHER RESPONSIBILITY MATTERS

By signing and submitting this bid or proposal, the prospective lower tier participant is providing the signed certification set out below.

1. It will comply and facilitate compliance with U.S. DOT regulations, “No procurement Suspension and Debarment,” 2 CFR part 1200, which adopts and supplements the U.S. Office of Management and Budget (U.S. OMB) “Guidelines to Agencies on Governmentwide Debarment and Suspension (No procurement),” 2 CFR part 180,

2. To the best of its knowledge and belief, that its Principals and Subrecipients at the first tier:
   a. Are eligible to participate in covered transactions of any Federal department or agency and are not presently: debarred, suspended, proposed for debarment, declared ineligible, voluntarily excluded, or disqualified
   b. Its management has not within a three-year period preceding its latest application or proposal been convicted of or had a civil judgment rendered against any of them for:
      1. Commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction, or contract under a public transaction,
      2. Violation of any Federal or State antitrust statute, or
      3. Proposed for debarment commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making any false statement, or receiving stolen property
   c. It is not presently indicted for, or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses listed in the preceding subsection 2.b of this Certification,
   d. It has not had one or more public transactions (Federal, State, or local) terminated for cause or default within a three-year period preceding this Certification,
   e. If, at a later time, it receives any information that contradicts the statements of subsections 2.a – 2.d above, it will promptly provide that information to FTA,
   f. It will treat each lower tier contract or lower tier subcontract under its Project as a covered lower tier contract for purposes of 2 CFR part 1200 and 2 CFR part 180 if it:
      1. Equals or exceeds $25,000,
      2. Is for audit services, or
      3. Requires the consent of a Federal official, and
   g. It will require that each covered lower tier contractor and subcontractor:
      1. Comply and facilitate compliance with the Federal requirements of 2 CFR parts 180 and 1200, and
      2. Assure that each lower tier participant in its Project is not presently declared by any Federal department or agency to be:
         a. Debarred from participation in its federally funded Project,
         b. Suspended from participation in its federally funded Project,
c. Proposed for debarment from participation in its federally funded Project,
d. Declared ineligible to participate in its federally funded Project,
e. Voluntarily excluded from participation in its federally funded Project, or
f. Disqualified from participation in its federally funded Project, and

3. It will provide a written explanation as indicated on a page attached in FTA’s TrAMSWeb or the
Signature Page if it or any of its principals, including any of its first tier Subrecipients or its Third-Party
Participants at a lower tier, is unable to certify compliance with the preceding statements in this
Certification Group.

_________________________________________ certifies or affirms the truthfulness and accuracy
of the contents of the statements submitted on or with this certification and understands that the
provisions of 31 U.S.C. Section 3801 ET SEQ. are applicable thereto.

Signature of Authorized Official

_________________________________________
Title

_________________________________________
Date
EXHIBIT D
CERTIFICATION OF RESTRICTIONS ON LOBBYING

I, _________________________________________________, hereby certify

(Name and title of official)

On behalf of ______________________________________________ that:

(Name of Bidder(s)/Company Name)

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

⮚ If any funds other than federal appropriated funds have been paid or will be paid to any person influencing or attempting to influence an officer or employee of any agency, a Member of Congress, and officer or employee of Congress, or an employee of a Member of Congress in connection with the federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form – LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

⮚ The undersigned shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including sub-contracts, subgrants and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by 31 U.S.C. § 1352 (as amended by the Lobbying Disclosure Act of 1995). Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

The undersigned certifies or affirms the truthfulness and accuracy of the contents of the statements submitted on or with this certification and understands that the provisions of 31 U.S.C. Section 3801, et seq., are applicable thereto.

Executed this ____ day of __________________, 20__.

____________________________________
Signature of Authorized Official

____________________________________
Signature of Notary and SEAL
Exhibit E

FTA Clauses

ACCESS TO RECORDS AND REPORTS

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

b. Retention Period. The Contractor agrees to comply with the record retention requirements in accordance with 2 C.F.R. § 200.333. The Contractor shall maintain all books, records, accounts and reports required under this Contract for a period of at least three (3) years after the date of termination or expiration of this Contract, except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case records shall be maintained until the disposition of all such litigation, appeals, claims or exceptions related thereto.

c. Access to Records. The Contractor agrees to provide sufficient access to FTA and its contractors to inspect and audit records and information related to performance of this contract as reasonably may be required.

d. Access to the Sites of Performance. The Contractor agrees to permit FTA and its contractors’ access to the sites of performance under this contract as reasonably may be required.

AMERICANS WITH DISABILITIES ACT (ADA)

The contractor agrees to comply with the requirements of 49 U.S.C. § 5301 (d), which states the Federal policy that the elderly and persons with disabilities have the same right as other persons to use mass transportation service and facilities, and that special efforts shall be made in planning and designing those services and facilities to implement that policy. The contractor also agrees to comply with all applicable requirements of section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794, which prohibits discrimination on the basis of handicaps, with the Americans with Disabilities Act of 1990 (ADA), as amended, 42 U.S.C. §§ 12101 et seq., which requires that accessible facilities and services be made available to persons with disabilities, including any subsequent amendments to that Act, and with the Architectural Barriers act of 1968, as amended, 42 U.S.C. §§ 4151 et seq., which requires that buildings and public accommodations be accessible to persons with disabilities, including any subsequent amendments to that Act. In addition, the contractor agrees to comply with any and all applicable requirements issued by the FTA, DOT, DOJ, U.S. GSA, U.S. EEOC, U.S. FCC, any subsequent amendments thereto and any other nondiscrimination statute(s) that may apply to the Project.

BYRD ANTI-LOBBYING AMENDMENT

Contractors who apply or bid for an award of $100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the Agency.”

CIVIL RIGHTS LAWS AND REGULATIONS

The following Federal Civil Rights laws and regulations apply to all contracts.

1. Federal Equal Employment Opportunity (EEO) Requirements. These include, but are not limited to:
a) Nondiscrimination in Federal Public Transportation Programs. 49 U.S.C. § 5332, covering projects, programs, and activities financed under 49 U.S.C. Chapter 53, prohibits discrimination on the basis of race, color, religion, national origin, sex (including sexual orientation and gender identity), disability, or age, and prohibits discrimination in employment or business opportunity.


Federal Protections for Individuals with Disabilities. The Americans with Disabilities Act of 1990, as amended (ADA), 42 U.S.C. § 12101 et seq., prohibits discrimination against qualified individuals with disabilities in programs, activities, and services, and imposes specific requirements on public and private entities. Third party contractors must comply with their responsibilities under Titles I, II, III, IV, and V of the ADA in employment, public services, public accommodations, telecommunications, and other provisions, many of which are subject to regulations issued by other Federal agencies.

Civil Rights and Equal Opportunity

The Agency is an Equal Opportunity Employer. As such, the Agency agrees to comply with all applicable Federal civil rights laws and implementing regulations. Apart from inconsistent requirements imposed by Federal laws or regulations, the Agency agrees to comply with the requirements of 49 U.S.C. § 5323(h)(3) by not using any Federal assistance awarded by FTA to support procurements using exclusionary or discriminatory specifications. Under this Contract, the Contractor shall at all times comply with the following requirements and shall include these requirements in each subcontract entered into as part thereof.

1. Nondiscrimination. In accordance with Federal transit law at 49 U.S.C. § 5332, the Contractor agrees that it will not discriminate against any employee or applicant for employment because of race, color, religion, national origin, sex, disability, or age. In addition, the Contractor agrees to comply with applicable Federal implementing regulations and other implementing requirements FTA may issue.

2. Race, Color, Religion, National Origin, Sex. In accordance with Title VII of the Civil Rights Act, as amended, 42 U.S.C. § 2000e et seq., and Federal transit laws at 49 U.S.C. § 5332, the Contractor agrees to comply with all applicable equal employment opportunity requirements of U.S. Department of Labor (U.S. DOL) regulations, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," 41 C.F.R. chapter 60, and Executive Order No. 11246, "Equal Employment Opportunity in Federal Employment," September 24, 1965, 42 U.S.C. § 2000e note, as amended by any later Executive Order that amends or supersedes it, referenced in 42 U.S.C. § 2000e note. The Contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, national origin, or sex (including sexual orientation and gender identity). Such action shall include, but not be limited to, the
following: employment, promotion, demotion or transfer, recruitment or recruitment advertising, layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. In addition, the Contractor agrees to comply with any implementing requirements FTA may issue.


5. **Promoting Free Speech and Religious Liberty.** The Contractor shall ensure that Federal funding is expended in full accordance with the U.S. Constitution, Federal Law, and statutory and public policy requirements: including, but not limited to, those protecting free speech, religious liberty, public welfare, the environment, and prohibiting discrimination.

**CLEAN AIR ACT AND FEDERAL WATER POLLUTION CONTROL ACT**

The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. § 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. § 1251-1387). Violations must be reported to FTA and the Regional Office of the Environmental Protection Agency. The following applies for contracts of amounts in excess of $150,000:

1. The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

2. The contractor agrees to report each violation to the Agency and understands and agrees that the Agency will, in turn, report each violation as required to assure notification to the Agency, Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

3. The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FTA.

**Federal Water Pollution Control Act**

1. The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

2. The contractor agrees to report each violation to the Agency and understands and agrees that the Agency will, in turn, report each violation as required to assure notification to the Agency, Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

3. The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FTA.

**CONFORMANCE WITH ITS NATIONAL ARCHITECTURE**
Intelligent Transportation Systems (ITS) projects shall conform to the National ITS Architecture and standards. Conformance with the National ITS Architecture is interpreted to mean the use of the National ITS Architecture to develop a regional ITS architecture in support of integration and the subsequent adherence of all ITS projects to that regional ITS architecture. Development of the regional ITS architecture should be consistent with the transportation planning process for Statewide and Metropolitan Transportation Planning (49 CFR Part 613 and 621).

DEBARMENT AND SUSPENSION

a. Applicability: This requirement applies to all FTA grant and cooperative agreement programs for a contract in the amount of at least $25,000

(1) This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such the contractor is required to verify that none of the contractor, its principals (defined at 2 C.F.R. § 180.995), or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(2) C.F.R. pt. 3000, subpart C and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(3) The accompanying certification is a material representation of fact relied upon by the subrecipient. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the Agency and subrecipient, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

DISADVANTAGED BUSINESS ENTERPRISE (DBE)

The contractor or subcontractor shall not discriminate on the basis of race, color, national origin, or sex in the performance of this contract. The contractor shall carry out applicable requirements of 49 C.F.R. part 26 in the award and administration of DOT assisted contracts. Failure by the contractor to carry out these requirements is a material breach of this contract, which may result in the termination of this contract or such other remedy as the Agency deems appropriate, which may include, but is not limited to:

(1) Withholding monthly progress payments;
(2) Assessing sanctions;
(3) Liquidated damages; and/or
(4) Disqualifying the contractor from future bidding as non-responsible. 49 C.F.R. § 26.13(b).

Prime contractors are required to pay subcontractors for satisfactory performance of their contracts no later than 30 days from receipt of each payment the Agency makes to the prime contractor. 49 C.F.R. § 26.29(a).

Finally, for contracts with defined DBE contract goals, each FTA Recipient must include in each prime contract a provision stating that the contractor shall utilize the specific DBEs listed unless the contractor obtains the Agency’s written consent; and that, unless the Agency’s consent is provided, the contractor shall not be entitled to any payment for work or material unless it is performed or supplied by the listed DBE. 49 C.F.R. § 26.53(f) (1).
It is the policy of the Agency and the United States Department of Transportation ("DOT") that Disadvantaged Business Enterprises ("DBE’s"), as defined herein and in the Federal regulations published at 49 C.F.R. part 26, shall have an equal opportunity to participate in DOT assisted contracts.

ENERGY CONSERVATION

The contractor agrees to comply with mandatory standards and policies relating to energy efficiency, which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act.

EQUAL EMPLOYMENT OPPORTUNITY

During the performance of this contract, the contractor agrees as follows:

(1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: 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. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

(2) The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

(4) The contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under section 202 of Executive Order 11246 of September 24, 1965, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the contracting agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the contractor's non-compliance with the nondiscrimination clauses of this contract or with any of such rules, regulations, or orders, this contract may be canceled, terminated or suspended in
whole or in part and the contractor may be declared ineligible for further Government contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The contractor will include the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as may be directed by the Secretary of Labor as a means of enforcing such provisions including sanctions for noncompliance: Provided, however, that in the event the contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

FEDERAL CHANGES

49 CFR Part 18 Federal Changes - Contractor shall at all times comply with all applicable FTA regulations, policies, procedures and directives, including without limitation those listed directly or by reference in the Master Agreement between Purchaser and FTA, as they may be amended or promulgated from time to time during the term of this contract. Contractor's failure to so comply shall constitute a material breach of this contract.

FLY AMERICA

a) Definitions. As used in this clause—
   1) "International air transportation" means transportation by air between a place in the United States and a place outside the United States or between two places both of which are outside the United States. 2) "United States" means the 50 States, the District of Columbia, and outlying areas. 3) "U.S.-flag air carrier" means an air carrier holding a certificate under 49 U.S.C. Chapter 411.

b) When Federal funds are used to fund travel, Section 5 of the International Air Transportation Fair Competitive Practices Act of 1974 (49 U.S.C. 40118) (Fly America Act) requires contractors, Agencys, and others use U.S.-flag air carriers for U.S. Government financed international air transportation of personnel (and their personal effects) or property, to the extent that service by those carriers is available. It requires the Comptroller General of the United States, in the absence of satisfactory proof of the necessity for foreign flag air transportation, to disallow expenditures from funds, appropriated or otherwise established for the account of the United States, for international air transportation secured aboard a foreign flag air carrier if a U.S.-flag air carrier is available to provide such services.

c) If available, the Contractor, in performing work under this contract, shall use U.S.-flag carriers for international air transportation of personnel (and their personal effects) or property.

d) In the event that the Contractor selects a carrier other than a U.S.-flag air carrier for international air transportation, the Contractor shall include a statement on vouchers involving such transportation essentially as follows:

   Statement of Unavailability of U.S.-Flag Air Carriers
   International air transportation of persons (and their personal effects) or property by U.S.-flag air carrier was not available or it was necessary to use foreign flag air carrier service for the following reasons. See FAR § 47.403.

e) Contractor shall include the substance of this clause, including this paragraph (e), in each subcontract or purchase under this contract that may involve international air transportation.

INCORPORATION OF FEDERAL TRANSIT ADMINISTRATION (FTA) TERMS
Incorporation of Federal Transit Administration (FTA) Terms - The provisions within include, in part, certain Standard Terms and Conditions required by DOT, whether or not expressly set forth in the preceding contract provisions. All contractual provisions required by DOT, as set forth in the current FTA Circular 4220 are hereby incorporated by reference. Anything to the contrary herein notwithstanding, all FTA mandated terms shall be deemed to control in the event of a conflict with other provisions contained in this Contract. The Contractor shall not perform any act, fail to perform any act, or refuse to comply with any request which would cause a violation of the FTA terms and conditions.

NO GOVERNMENT OBLIGATION TO THIRD PARTIES

The Agency and Contractor acknowledge and agree that, notwithstanding any concurrence by the Federal Government in or approval of the solicitation or award of the underlying Contract, absent the express written consent by the Federal Government, the Federal Government is not a party to this Contract and shall not be subject to any obligations or liabilities to the Agency, Contractor or any other party (whether or not a party to that contract) pertaining to any matter resulting from the underlying Contract. The Contractor agrees to include the above clause in each subcontract financed in whole or in part with Federal assistance provided by the FTA. It is further agreed that the clause shall not be modified, except to identify the subcontractor who will be subject to its provisions.

NOTIFICATION TO FTA

If a current or prospective legal matter that may affect the Federal Government emerges, the Recipient must promptly notify the FTA Chief Counsel and FTA Regional Counsel for the Region in which the Recipient is located. The Recipient must include a similar notification requirement in its Third Party Agreements and must require each Third Party Participant to include an equivalent provision in its subagreements at every tier, for any agreement that is a “covered transaction” according to 2 C.F.R. §§ 180.220 and 1200.220.

(1) The types of legal matters that require notification include, but are not limited to, a major dispute, breach, default, litigation, or naming the Federal Government as a party to litigation or a legal disagreement in any forum for any reason.

(2) Matters that may affect the Federal Government include, but are not limited to, the Federal Government’s interests in the Award, the accompanying Underlying Agreement, and any Amendments thereto, or the Federal Government’s administration or enforcement of federal laws, regulations, and requirements.

(3) The Recipient must promptly notify the U.S. DOT Inspector General in addition to the FTA Chief Counsel or Regional Counsel for the Region in which the Recipient is located, if the Recipient has knowledge of potential fraud, waste, or abuse occurring on a Project receiving assistance from FTA. The notification provision applies if a person has or may have submitted a false claim under the False Claims Act, 31 U.S.C. § 3729 et seq., or has or may have committed a criminal or civil violation of law pertaining to such matters as fraud, conflict of interest, bribery, gratuity, or similar misconduct. This responsibility occurs whether the Project is subject to this Agreement or another agreement between the Recipient and FTA, or an agreement involving a principal, officer, employee, agent, or Third Party Participant of the Recipient. It also applies to subcontractors at any tier. Knowledge, as used in this paragraph, includes, but is not limited to, knowledge of a criminal or civil investigation by a Federal, state, or local law enforcement or other investigative agency, a criminal indictment or civil complaint, or probable cause that could support a criminal indictment, or any other credible information in the possession of the Recipient.

PATENT RIGHTS AND RIGHTS IN DATA

Intellectual Property Rights
This Project is funded through a Federal award with FTA for experimental, developmental, or research work purposes. As such, certain Patent Rights and Data Rights apply to all subject data first produced in the performance of this Contract. The Contractor shall grant the Agency intellectual property access and licenses deemed necessary for the work performed under this Contract and in accordance with the requirements of 37 C.F.R. part 401, “Rights to Inventions Made by Nonprofit Organizations and Small
Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by FTA or U.S. DOT. The terms of an intellectual property agreement and software license rights will be finalized prior to execution of this Contract and shall, at a minimum, include the following restrictions:

Except for its own internal use, the Contractor may not publish or reproduce subject data in whole or in part, or in any manner or form, nor may the Contractor authorize others to do so, without the written consent of FTA, until such time as FTA may have either released or approved the release of such data to the public. This restriction on publication, however, does not apply to any contract with an academic institution. For purposes of this Contract, the term “subject data” means recorded information whether or not copyrighted, and that is delivered or specified to be delivered as required by the Contract. Examples of “subject data” include, but are not limited to computer software, standards, specifications, engineering drawings and associated lists, process sheets, manuals, technical reports, catalog item identifications, and related information, but do not include financial reports, cost analyses, or other similar information used for performance or administration of the Contract.

1. The Federal Government reserves a royalty-free, non-exclusive and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use for “Federal Government Purposes,” any subject data or copyright described below. For “Federal Government Purposes,” means use only for the direct purposes of the Federal Government. Without the copyright owner’s consent, the Federal Government may not extend its Federal license to any other party.

   a. Any subject data developed under the Contract, whether or not a copyright has been obtained; and
   b. Any rights of copyright purchased by the Contractor using Federal assistance in whole or in part by the FTA.

2. Unless FTA determines otherwise, the Contractor performing experimental, developmental, or research work required as part of this Contract agrees to permit FTA to make available to the public, either FTA’s license in the copyright to any subject data developed in the course of the Contract, or a copy of the subject data first produced under the Contract for which a copyright has not been obtained. If the experimental, developmental, or research work, which is the subject of this Contract, is not completed for any reason whatsoever, all data developed under the Contract shall become subject data as defined herein and shall be delivered as the Federal Government may direct.

3. Unless prohibited by state law, upon request by the Federal Government, the Contractor agrees to indemnify, save, and hold harmless the Federal Government, its officers, agents, and employees acting within the scope of their official duties against any liability, including costs and expenses, resulting from any willful or intentional violation by the Contractor of proprietary rights, copyrights, or right of privacy, arising out of the publication, translation, reproduction, delivery, use, or disposition of any data furnished under that contract. The Contractor shall be required to indemnify the Federal Government for any such liability arising out of the wrongful act of any employee, official, or agents of the Federal Government.

4. Nothing contained in this clause on rights in data shall imply a license to the Federal Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Federal Government under any patent.

5. Data developed by the Contractor and financed entirely without using Federal assistance provided by the Federal Government that has been incorporated into work required by the underlying Contract is exempt from the requirements herein, provided that the Contractor identifies those data in writing at the time of delivery of the Contract work.

6. The Contractor agrees to include these requirements in each subcontract for experimental, developmental, or research work financed in whole or in part with Federal assistance.
PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS AND RELATED ACTS

The contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the contractor’s actions pertaining to this contract.

PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

a. Recipients and subrecipients are prohibited from obligating or expending loan or grant funds to:
   1. Procure or obtain;
   2. Extend or renew a contract to procure or obtain;
   or
   3. Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
      i. For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
      ii. Telecommunications or video surveillance services provided by such entities or using such equipment.
      iii. Telecommunications or video surveillance equipment or services procured or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

b. In implementing the prohibition under Public Law 115-232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

c. See Public Law 115-232, section 889 for additional information.

d. See also § 200.471.

PROMPT PAYMENT

The contractor is required to pay its subcontractors performing work related to this contract for satisfactory performance of that work no later than 30 days after the contractor’s receipt of payment for that work. In addition, the contractor is required to return any retainage payments to those subcontractors within 30 days after the subcontractor's work related to this contract is satisfactorily completed.

The contractor must promptly notify the Agency, whenever a DBE subcontractor performing work related to this contract is terminated or fails to complete its work and must make good faith efforts to engage another DBE subcontractor to perform at least the same amount of work. The contractor may not terminate any DBE subcontractor and perform that work through its own forces or those of an affiliate without prior written consent of the Agency.

SAFE OPERATION OF MOTOR VEHICLES

Seat Belt Use
The Contractor is encouraged to adopt and promote on-the-job seat belt use policies and programs for its employees and other personnel that operate company owned vehicles, company rented vehicles, or personally operated vehicles. The terms “company owned” and “company leased” refer to vehicles owned or leased either by the Contractor or Agency.
Distracted Driving
The Contractor agrees to adopt and enforce workplace safety policies to decrease crashes caused by
distracted drivers, including policies to ban text messaging while using an electronic device supplied by
an employer, and driving a vehicle the driver owns or rents, a vehicle Contractor owns, leases, or rents, or
a privately owned vehicle when on official business in connection with the work performed under this
Contract.

SEISMIC SAFETY
The contractor agrees that any new building or addition to an existing building will be designed and
constructed in accordance with the standards for Seismic Safety required in Department of Transportation
(DOT) Seismic Safety Regulations 49 C.F.R. part 41 and will certify to compliance to the extent required
by the regulation. The contractor also agrees to ensure that all work performed under this contract,
including work performed by a subcontractor, is in compliance with the standards required by the Seismic
Safety regulations and the certification of compliance issued on the project.

SIMPLIFIED ACQUISITION THRESHOLD
Contracts for more than the simplified acquisition threshold, which is the inflation adjusted amount
determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council
(Councils) as authorized by 41 U.S.C. § 1908, or otherwise set by law, must address administrative,
contractual, or legal remedies in instances where contractors violate or breach contract terms, and
provide for such sanctions and penalties as appropriate. (Note that the simplified acquisition threshold
determines the procurement procedures that must be employed pursuant to 2 C.F.R. §§ 200.317–
200.327. The simplified acquisition threshold does not exempt a procurement from other eligibility or
processes requirements that may apply. For example, Buy America’s eligibility and process requirements
apply to any procurement in excess of $150,000. 49 U.S.C. § 5323(j)(13).

SPECIAL NOTIFICATION REQUIREMENTS FOR STATES
Applies to States –

a. To the extent required under federal law, the State, as the Recipient, agrees to provide the following
information about federal assistance awarded for its State Program, Project, or related activities:

(1) The Identification of FTA as the federal agency providing the federal assistance for a State Program or
Project;
(2) The Catalog of Federal Domestic Assistance Number of the program from which the federal
assistance for a State Program or Project is authorized; and
(3) The amount of federal assistance FTA has provided for a State Program or Project.

b. Documents - The State agrees to provide the information required under this provision in the following
documents: (1) applications for federal assistance, (2) requests for proposals or solicitations, (3) forms,
(4) notifications, (5) press releases, and (6) other publications.

TERMINATION
Termination for Convenience (General Provision)
The Agency may terminate this contract, in whole or in part, at any time by written notice to the Contractor
when it is in the Agency’s best interest. The Contractor shall be paid its costs, including contract close-out
costs, and profit on work performed up to the time of termination. The Contractor shall promptly submit its
termination claim to Agency to be paid the Contractor. If the Contractor has any property in its possession
belonging to Agency, the Contractor will account for the same, and dispose of it in the manner Agency
directs.

Termination for Default [Breach or Cause] (General Provision)
If the Contractor does not deliver supplies in accordance with the contract delivery schedule, or if the
contract is for services, the Contractor fails to perform in the manner called for in the contract, or if the
Contractor fails to comply with any other provisions of the contract, the Agency may terminate this
contract for default. Termination shall be effected by serving a Notice of Termination on the Contractor setting forth the manner in which the Contractor is in default. The Contractor will be paid only the contract price for supplies delivered and accepted, or services performed in accordance with the manner of performance set forth in the contract. If it is later determined by the Agency that the Contractor had an excusable reason for not performing, such as a strike, fire, or flood, events which are not the fault of or are beyond the control of the Contractor, the Agency, after setting up a new delivery of performance schedule, may allow the Contractor to continue work, or treat the termination as a Termination for Convenience.

Opportunity to Cure (General Provision)
The Agency, in its sole discretion may, in the case of a termination for breach or default, allow the Contractor [an appropriately short period of time] in which to cure the defect. In such case, the Notice of Termination will state the time period in which cure is permitted and other appropriate conditions.

If Contractor fails to remedy to Agency's satisfaction the breach or default of any of the terms, covenants, or conditions of this Contract within [10 days] after receipt by Contractor of written notice from Agency setting forth the nature of said breach or default, Agency shall have the right to terminate the contract without any further obligation to Contractor. Any such termination for default shall not in any way operate to preclude Agency from also pursuing all available remedies against Contractor and its sureties for said breach or default.

Waiver of Remedies for any Breach
In the event that Agency elects to waive its remedies for any breach by Contractor of any covenant, term or condition of this contract, such waiver by Agency shall not limit Agency's remedies for any succeeding breach of that or of any other covenant, term, or condition of this contract.

Termination for Convenience (Professional or Transit Service Contracts)
The Agency, by written notice, may terminate this contract, in whole or in part, when it is in the Agency’s interest. If this contract is terminated, the Agency shall be liable only for payment under the payment provisions of this contract for services rendered before the effective date of termination.

Termination for Default (Supplies and Service)
If the Contractor fails to deliver supplies or to perform the services within the time specified in this contract or any extension, or if the Contractor fails to comply with any other provisions of this contract, the Agency may terminate this contract for default. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature of the default. The Contractor will only be paid the contract price for supplies delivered and accepted, or services performed in accordance with the manner or performance set forth in this contract. If, after termination for failure to fulfill contract obligations, it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Agency.

Termination for Default (Transportation Services)
If the Contractor fails to pick up the commodities or to perform the services, including delivery services, within the time specified in this contract or any extension, or if the Contractor fails to comply with any other provisions of this contract, the Agency may terminate this contract for default. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature of default. The Contractor will only be paid the contract price for services performed in accordance with the manner of performance set forth in this contract.

If this contract is terminated while the Contractor has possession of Agency goods, the Contractor shall, upon direction of the Agency, protect and preserve the goods until surrendered to the Agency or its agent. The Contractor and Agency shall agree on payment for the preservation and protection of goods. Failure to agree on an amount will be resolved under the Dispute clause.
If, after termination for failure to fulfill contract obligations, it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Agency.

Termination for Default (Construction)
If the Contractor refuses or fails to prosecute the work or any separable part, with the diligence that will ensure its completion within the time specified in this contract or any extension or fails to complete the work within this time, or if the Contractor fails to comply with any other provision of this contract, Agency may terminate this contract for default. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature of the default. In this event, the Agency may take over the work and compete it by contract or otherwise, and may take possession of and use any materials, appliances, and plant on the work site necessary for completing the work. The Contractor and its sureties shall be liable for any damage to the Agency resulting from the Contractor's refusal or failure to complete the work within specified time, whether or not the Contractor's right to proceed with the work is terminated. This liability includes any increased costs incurred by the Agency in completing the work.

The Contractor's right to proceed shall not be terminated nor shall the Contractor be charged with damages under this clause if: 1. The delay in completing the work arises from unforeseeable causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include: acts of God, acts of Agency, acts of another contractor in the performance of a contract with Agency, epidemics, quarantine restrictions, strikes, freight embargoes; and 2. The Contractor, within [10] days from the beginning of any delay, notifies Agency in writing of the causes of delay. If, in the judgment of Agency, the delay is excusable, the time for completing the work shall be extended. The judgment of Agency shall be final and conclusive for the parties, but subject to appeal under the Disputes clause(s) of this contract. 3. If, after termination of the Contractor's right to proceed, it is determined that the Contractor was not in default, or that the delay was excusable, the rights and obligations of the parties will be the same as if the termination had been issued for the convenience of Agency.

Termination for Convenience or Default (Architect and Engineering)
The Agency may terminate this contract in whole or in part, for the Agency's convenience or because of the failure of the Contractor to fulfill the contract obligations. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature, extent, and effective date of the termination. Upon receipt of the notice, the Contractor shall (1) immediately discontinue all services affected (unless the notice directs otherwise), and (2) deliver to the Agency's Contracting Officer all data, drawings, specifications, reports, estimates, summaries, and other information and materials accumulated in performing this contract, whether completed or in process. Agency has a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, all such data, drawings, specifications, reports, estimates, summaries, and other information and materials.

If the termination is for the convenience of the Agency, the Agency's Contracting Officer shall make an equitable adjustment in the contract price but shall allow no anticipated profit on unperformed services.

If the termination is for failure of the Contractor to fulfill the contract obligations, the Agency may complete the work by contract or otherwise and the Contractor shall be liable for any additional cost incurred by the Agency.

If, after termination for failure to fulfill contract obligations, it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of Agency.

Termination for Convenience or Default (Cost-Type Contracts)
The Agency may terminate this contract, or any portion of it, by serving a Notice of Termination on the Contractor. The notice shall state whether the termination is for convenience of Agency or for the default of the Contractor. If the termination is for default, the notice shall state the manner in which the Contractor has failed to perform the requirements of the contract. The Contractor shall account for any property in its possession paid for from funds received from the Agency, or property supplied to the Contractor by the Agency. If the termination is for default, the Agency may fix the fee, if the contract provides for a fee, to be
paid the Contractor in proportion to the value, if any, of work performed up to the time of termination. The Contractor shall promptly submit its termination claim to the Agency and the parties shall negotiate the termination settlement to be paid the Contractor.

If the termination is for the convenience of Agency, the Contractor shall be paid its contract close-out costs, and a fee, if the contract provided for payment of a fee, in proportion to the work performed up to the time of termination.

If, after serving a Notice of Termination for Default, the Agency determines that the Contractor has an excusable reason for not performing, the Agency, after setting up a new work schedule, may allow the Contractor to continue work, or treat the termination as a Termination for Convenience.

VIOLATION AND BREACH OF CONTRACT

Rights and Remedies of the Agency

The Agency shall have the following rights in the event that the Agency deems the Contractor guilty of a breach of any term under the Contract.

1. The right to take over and complete the work or any part thereof as agency for and at the expense of the Contractor, either directly or through other contractors; 2. The right to cancel this Contract as to any or all of the work yet to be performed; 3. The right to specific performance, an injunction or any other appropriate equitable remedy; and 4. The right to money damages.

For purposes of this Contract, breach shall include.

Rights and Remedies of Contractor

Inasmuch as the Contractor can be adequately compensated by money damages for any breach of this Contract, which may be committed by the Agency, the Contractor expressly agrees that no default, act or omission of the Agency shall constitute a material breach of this Contract, entitling Contractor to cancel or rescind the Contract (unless the Agency directs Contractor to do so) or to suspend or abandon performance.

Remedies

Substantial failure of the Contractor to complete the Project in accordance with the terms of this Contract will be a default of this Contract. In the event of a default, the Agency will have all remedies in law and equity, including the right to specific performance, without further assistance, and the rights to termination or suspension as provided herein. The Contractor recognizes that in the event of a breach of this Contract by the Contractor before the Agency takes action contemplated herein, the Agency will provide the Contractor with sixty (60) days written notice that the Agency considers that such a breach has occurred and will provide the Contractor a reasonable period of time to respond and to take necessary corrective action.

Disputes

Disputes arising in the performance of this Contract that are not resolved by agreement of the parties shall be decided in writing by an authorized representative of Agency. This decision shall be final and conclusive unless within [10] days from the date of receipt of its copy, the Contractor mails or otherwise furnishes a written appeal to the Agency's authorized representative. In connection with any such appeal, the Contractor shall be afforded an opportunity to be heard and to offer evidence in support of its position. The decision of the Agency's authorized representative shall be binding upon the Contractor and the Contractor shall abide by the decision.

In the event that a resolution of the dispute is not mutually agreed upon, the parties can agree to mediate the dispute or proceed with litigation. Notwithstanding any provision of this section, or any other provision of this Contract, it is expressly agreed and understood that any court proceeding arising out of a dispute under the Contract shall be heard by a Court de novo and the court shall not be limited in such
proceeding to the issue of whether the Authority acted in an arbitrary, capricious or grossly erroneous manner.

Pending final settlement of any dispute, the parties shall proceed diligently with the performance of the Contract, and in accordance with the Agency’s direction or decisions made thereof.

Performance during Dispute
Unless otherwise directed by Agency, Contractor shall continue performance under this Contract while matters in dispute are being resolved.

Claims for Damages
Should either party to the Contract suffer injury or damage to person or property because of any act or omission of the party or of any of its employees, agents or others for whose acts it is legally liable, a claim for damages therefor shall be made in writing to such other party within a reasonable time after the first observance of such injury or damage.

Remedies
Unless this Contract provides otherwise, all claims, counterclaims, disputes and other matters in question between the Agency and the Contractor arising out of or relating to this Contract or its breach will be decided by arbitration if the parties mutually agree, or in a court of competent jurisdiction within the State in which the Agency is located.

Rights and Remedies
The duties and obligations imposed by the Contract documents and the rights and remedies available thereunder shall be in addition to and not a limitation of any duties, obligations, rights and remedies otherwise imposed or available by law. No action or failure to act by the Agency or Contractor shall constitute a waiver of any right or duty afforded any of them under the Contract, nor shall any such action or failure to act constitute an approval of or acquiescence in any breach thereunder, except as may be specifically agreed in writing.
Exhibit F – TCSDS Specifications & Scope of Work

1 Introduction
These specifications define the functional, performance, installation, integration and project implementation requirements for the deployment of trip coordination scheduling and dispatching software (TCTCSDS) for demand-response services that are operated by several agencies in Ohio Human Services Transportation Coordination (HSTC) Region 9. This document includes the following sections:

- Section 2 provides an overview of Mobility Ohio, services in HSTC Region 9, and the technical scope of this project, including a description of the user needs that resulted in these specifications;

- Section 3 defines the information technology (IT) requirements;

- Section 4 defines wireless data communication system requirements;

- Section 5 defines the geographic information system (GIS) and mapping requirements for the TCSDS;

- Section 6 defines the TCSDS system requirements;

- Section 7 defines the customer facing system requirements;

- Section 8 defines reporting requirements;

- Section 9 defines the functional and performance requirements for computer-sided dispatch (CAD) / automatic vehicle location (AVL);

- Section 10 defines optional and future needs;

- Section 11 defines the project implementation requirements;

- Section 12 defines warranty and spares requirements;

- Appendix A contains the Price Proposal Form; and

- Appendix B contains the Compliance Matrix.

2 Overview
This procurement is based on the Mobility Ohio Regional Vision for Transportation Coordination, which is shown in Figure 1. As eligible travelers request trips, their trip requests go to the Regional Transportation Resource Center (RTRC) which contains the software being procured and described in these specifications. The RTRC assigns each trip to an appropriate transportation provider based on a number of factors which will be described in Section 6. The figure shows three types of transportation providers (TPs), but there is another way to categorize the providers that we will use in this specification:
• **Open-Door TP**: TP that accepts any client referred to them through one or more funding programs; and

• **Closed-Door TP**: TP that only transports their own clients.

Please note that a TP can be both open-door and closed-door since they could have specific vehicles or vehicle-hours in each category. Further, please note that a TP can be a taxi company. Figure 2 shows a high-level diagram that generally describes the way the system (described in these specifications) will operate.

Overall, these specifications identify functional requirements for the RTRC to perform the following:

• Provide an interface/portal for the five groups of software users - the RTRC, TPs, facilities (e.g., hospital, doctor’s office), funding agencies and trip-making customers/clients - to exchange data and information in order to describe and utilize specific parameters for trip booking, offering, scheduling, matching and assignment, and invoicing and reporting;

• Provide real-time and optimized trip scheduling based on trip requests, trip offering and acceptance, and other parameters such as vehicle and driver characteristics;

• Provide a mechanism for TPs to bill/invoice the RTRC;

• Provide a mechanism for funding agencies to enter/update client eligibility;

• Provide on-board driver terminals (e.g., tablets) for communication of manifests, messaging between drivers and dispatchers, and trip monitoring; and

• Assign trips to providers whose drivers and vehicles meet safety and quality standards specific to a client’s needs.

Potential future requirements include but are not limited to the following:

• Provide the ability to interface with other TCSDS systems that build client profiles (e.g., hospital systems, healthcare facilities, social service agencies. For example, if a hospital initiates a ride request for a discharged patient, the patient’s information (name, address, contact information, etc.) shall be imported into the RTRC TCSDS software automatically;

• Provide the ability to interface with a statewide registry of the eligibility of TPs, drivers, and vehicles to operate human service transportation for various funding programs; and

• Provide the ability to create and use a universal regional pass. For example, the TCSDS software could include an electronic fare payment subsystem that could be used by the transit systems in the pilot region (see below for an explanation of the pilot region).
Figure 1. Mobility Ohio Pilot: A Regional Vision for Transportation Coordination
Figure 2. High-Level System Operation
Detailed information about these requirements is described throughout these specifications. It is expected that the RTRC will be located initially in the Mobility Ohio pilot region, consisting of Guernsey, Muskingum, Tuscarawas, and Coshocton Counties in Ohio. The pilot region is a subset of HSTC Region 9. In 2018, a working group, comprised of representation from the Ohio Departments of Transportation, Medicaid, Job and Family Services, and the Governor’s Office on Health recommended a ten-region system of regionalized Human Services Transportation. ODOT has created new boundaries for Human Services Transportation Coordination (HSTC) based on a combination of travel movement in Ohio and Area Agency on Aging (AAA), Managed Care Organization (MCO), Metropolitan Planning Organization (MPO), and Rural Transportation Planning Organization (RTPO) boundaries. The regionalization of Ohio’s HSTC programs, including public transportation, will facilitate a more cost-effective use of available funding and take advantage of regional deployment of enhanced technologies for all of Ohio’s human services programs that utilize agency-sponsored and public transportation resources. HSTC Region 9 consists of nine Ohio counties: Belmont, Carroll, Coshocton, Guernsey, Harrison, Holmes, Jefferson, Muskingum, & Tuscarawas. There are approximately 40 transportation service providers or human service agencies that provide or contract transportation services within the pilot region. The public served includes seniors, people with disabilities, zero-vehicles families, low income individuals, unemployed, veterans, Medicaid-eligible individuals, people with a low English proficiency, and others. The organizations that most frequently provide human services transportation in the pilot region are listed by county in Table 1.

The Ohio Department of Transportation (ODOT) Office of Transit is providing funding to assist the region with implementing a transportation coordination pilot project (the “Mobility Ohio pilot”) that will use the TCSDS software. ODOT will procure the TCSDS software governed by these specifications. The RTRC will be operated by a local agency that is yet to be determined. Although it will be procured and funded by ODOT, the TCSDS software will be installed at the agency that operates the RTRC.

<table>
<thead>
<tr>
<th>Table 2. Regional Transportation Service Providers List (Subject to Change)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Coshocton County</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Guernsey County</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Muskingum County</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
3 Mobility Ohio Mission and Vision

Mobility Ohio is a multi-agency effort to improve the safety, access, and quality of Ohio’s health and human service transportation network while mitigating fraud by establishing a consistent and effective oversight structure and increasing inter-agency coordination.

The Mobility Ohio vision, as shown in Figure 3, is to address unmet transportation needs identified by stakeholders in the Ohio Statewide Transit Needs Study, Transportation Challenges for Ohioans with Disabilities Study, and the Ohio Mobility Transformation Study. The vision establishes administration of all health and human service transportation through a single agency across ODOT’s HSTC Regions.

4 Project Scope

This subsection summarizes the scope of this project, including a summary of the user needs that, in part, resulted in these specifications.

Table 2 shows the overall requirements that must be met by the proposed trip coordination, scheduling and dispatching (TCSDS) software. Detailed requirements for each function can be found in Section 6.

Figure 3. Mobility Ohio Vision
This page intentionally left blank.
<table>
<thead>
<tr>
<th>TPs/Vehicles ➔ Overall Requirements</th>
<th>Open-Door TPs/RTRC Dedicated Vehicles</th>
<th>Open-Door TPs/Non-Dedicated Vehicles</th>
<th>Closed-Door TPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interaction between RTRC and TP</td>
<td></td>
<td>3. The RTRC will offer the trip to one or more providers depending on certain criteria</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. TPs accept trips that they are eligible to provide</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Trips need to match up with driver/vehicle tiers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TPs’ vehicles are listed on the RTRC daily schedule by parameters:</td>
<td>4. The RTRC assigns trips</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Vehicle tier</td>
<td>5. TPs invoice the RTRC for the service they provide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. Driver tier</td>
<td>6. TPs submit service data reports to the RTRC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. Hours in service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h. Service area/zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trip Scheduling Process</td>
<td>3. Client/Client Representative requests trip from the RTRC</td>
<td>3. TPs communicate trip schedules to the RTRC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. The RTRC schedules client with a TP on the appropriate driver and vehicle tier</td>
<td>4. The RTRC authorizes funding for the scheduled trips</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: Schedules are optimized so TPs may not know the exact schedule until the day before or the day of the trip. Schedule optimization is conducted in real-time so that keeping dedicated vehicles full is a priority.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Client/Client Representative requests trip from the RTRC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. The RTRC will offer the trip to one or more providers depending on certain criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. TP schedules the trip on a non-dedicated vehicle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: Schedules are optimized in real-time so trips may disappear/reappear throughout the scheduling process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. After trips are accepted, the RTRC can view vehicles on the daily schedule but the non-RTRC activities of the vehicle are not visible.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TP Technology Requirements</td>
<td>Required:</td>
<td>Required:</td>
<td>Required:</td>
</tr>
<tr>
<td></td>
<td>• Scheduling and dispatching software with ongoing real-time connection to the RTRC</td>
<td>• Scheduling and dispatching software with ongoing real-time connection to the RTRC</td>
<td>• A closed-door provider can use a paper-based scheduling system if necessary</td>
</tr>
<tr>
<td></td>
<td>• On-board driver terminals (e.g., tablets)</td>
<td>• On-board driver terminals (e.g., tablets)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Desired but not required:</td>
<td>Desired but not required:</td>
<td>Desired but not required:</td>
</tr>
<tr>
<td></td>
<td>• Pre-trip/post-trip inspection module on driver terminals (for enforcement of that standard)</td>
<td>• Ability to make non-RTRC activities not available to any software users</td>
<td>• Ability to use RTRC web-based billing and reporting portal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pre-trip/post-trip inspection module on driver terminals (e.g., tablets)</td>
<td>• On-board driver terminals (e.g., tablets)</td>
</tr>
<tr>
<td>tablets)</td>
<td>Pre-trip/post-trip inspection module on driver terminals (e.g., tablets)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This page intentionally left blank.
5 Information Technology (IT) Requirements

6 General
The selected vendor, referred to as the “Contractor” in the rest of this document, shall provide the hardware and configuration details for installing the system (1) at the location identified by the RTRC (site installation approach). The RTRC does prefer a virtualized server if possible depending on specs and storage requirement needs as well as growth or (2) at a data center proposed by the Contractor or in the State of Ohio’s data center/Public Cloud tenant (hosted approach). The data center selected for installation of the system must be approved by the RTRC. Further, the location of the data center must abide by Ohio Executive Orders 2019-12D and 2022-02D (that the eventual Contractor and any of its subcontractors shall perform no services requested outside of the United States and is specifically prohibited from performing any service using Russian companies or institutions)1.

The software applications shall include context sensitive help capability.
The software applications must run fully in the user context and shall not require elevated permissions or administrative permissions on the desktop.
All software applications must utilize the Microsoft Operating System consistent with RTRC upgrades, patches and service packs on the servers and desktops. The following Microsoft products must be used:
- Microsoft Office Suite: 2021;
- Microsoft Windows Desktop Operating System (OS): Windows 10;
- Microsoft Windows Server 2022; and

All software applications must support role-based security.
The Contractor is required to notify the RTRC when new releases of software applications become available, and when current releases and related systems are no longer supported. The Contractor must comply with the RTRC’s change management process when making any changes to supported systems; these changes must be reported to the RTRC project manager. The Contractor shall implement a test environment, with all software components installed on parallel hardware at the RTRC or hosted environment, where software updates and configuration changes can be tested prior to being implemented in the production system. Any future updates or upgrades must be tested in the test environment before being implemented on production servers. All software upgrades or changes required by the Contractor must be made in an RTRC test environment and certified prior to moving into a production environment. Any on-board firmware changes must be tested first in a “bus-in-box” type test bench before installing them on vehicles.

7 Required Infrastructure

8 Hardware
The Proposer shall provide the specifications for hardware that comprises the proposed central system, including the required number of workstations for all users. Proposers shall provide the server hardware requirements required to support the proposed solution since the RTRC may

1 https://governor.ohio.gov/wps/portal/gov/governor/media/executive-orders
procure the hardware from a supplier other than the Contractor and may decide to use the site installation approach.
For site installation, the RTRC reserves the right to confirm the specifications of the Contractor-recommended and supplied hardware and the RTRC reserves the right to offer virtualization within the current infrastructure as a potential replacement for hardware.
The Proposer shall supply the specifications for workstations and tablets, which the RTRC may procure from suppliers other than the Contractor.

9 Software
The successful Contractor shall provide software and specifications for hardware that comprise the proposed central system, including the required number of licenses for all users. The cost of each component shall be provided per the instructions on the Price Proposal Form.
The Contractor shall provide their proposed system’s source code\(^2\) to the RTRC. ODOT ownership of the source is subject to the following requirements:

- ODOT is the owner of the source code being written;
- The solution should align with ODOT's technology stack - .NET Core 2.1 or newer / .NET Framework 4.0 or newer / C# / Angular / ExtJS / jQuery / Bootstrap / Log4Net;
- The Contractor must provide all source code to ODOT;
- Source code will be subject to code review. While ODOT will try to be reasonable, the Contractor must be willing to make necessary changes if ODOT finds the code to be unacceptable:
  - There should be a separation of layers;
  - Coding conventions and best practices should be followed;
  - Business logic code should be reasonably commented; and
  - Functioning unit tests should be provided; and

The Contractor cannot charge the State of Ohio for copies of the source code or backups of the data after it is located in the Contractor’s cloud.
The Contractor shall supply the specifications for workstations and monitors, which the RTRC will supply and/or procure.
For a hosted approach, the Proposer shall clearly define the approach for software hosting and access (e.g., Citrix’s independent computing architecture [ICA] protocol, Microsoft’s remote desktop protocol [RDP] over secure virtual private network (VPN) connection, completely web-based application accessible via hypertext transport protocol secure [HTTPS]) on standard web browsers (e.g., Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari).
The Proposer must identify the cloud platform that will be used (e.g., Amazon Cloud Services vs Microsoft Azure Cloud Services).
The Contractor shall implement a test environment, with all software components installed (1) on parallel server hardware at the RTRC (site installation) or (2) at the data center (hosted

---
\(^2\) "Source Code" means the source code, design and associated preliminary materials, object code, file formats and specifications, build and compilation scripts and instructions, databases, configuration data, audio, video, literal and other media and materials, including accompanying documentation relating to or comprising the software built by an ODOT contractor and is owned by ODOT.
installation), where software updates and configuration changes can be tested prior to being implemented in the production system. Any future updates or upgrades must be tested in the test environment before being implemented on production servers. All software upgrades or changes required by the Contractor must be made in the test environment and certified prior to moving into a production environment.

Using a hosted approach, at least two parallel data centers in two different geographic locations shall be utilized.

The Central system shall be setup in redundant configuration by default. So, if the primary application fails, the secondary application that is configured to run in hot-standby mode shall automatically start running as the primary application to ensure fail-safe operation. Each Proposer shall provide a clear description of their approach for enabling redundant server configuration.

For hosted solution, Proposers shall describe the minimum computer hardware and browser requirements (e.g., minimum Random Access Memory [RAM] requirements for map rendering, java run-time environment [JRE] for java-based web applications).

10 Information Security
The Contractor shall be asked to comply with best practices with all areas of IT Security as outlined by Health Insurance Portability and Accountability Act (HIPAA) rules. The RTRC has specific policies in the following areas, if you require additional information please contact the RTRC IT to discuss in more detail.

- Acceptable Use
- Automatic Log-Off
- Data Backup
- Emergency Access to EHR
- Encryption and Decryption
- IT Risk Management Program
- Malware Protection
- Password Management
- Portable Computing Device Privacy and Security
- Privacy and Security of Protected Health Information
- Termination of Access
- Transmission Security
- Unique User ID
- Workstation Use and Security
All software applications must support role-based security.

ODOT requires the Contractor to perform regular periodic (every six months or every year) Penetration (Pen Tests) tests and report the results.

The Contractor shall follow the RTRC IT Security Policies, which will be provided at a later date.

For a locally-installed solution, all software applications must have the ability to use Windows Authentication based upon Active Directory setup. For a hosted solution, please describe the administrative needs to add users to the system.

The methods used for encrypting stored passwords must be disclosed. Industry standard encryption methods utilizing at least 256 bit encryption techniques are required.

The Proposer must disclose provisions to secure the database in its proposal.

Any vulnerabilities or exploits discovered by the Contractor or others for the proposed application must be reported to the RTRC immediately with a proposed mitigation strategy.

The Contractor shall support Microsoft security patches and updates within fifteen (15) days of release.

The system must track all activities performed by software users for auditing purposes (e.g., system configuration changes, trip booking, modifications and client data editing).

The methods used for encrypting stored passwords must be disclosed. Industry standard encryption methods utilizing at least 256 bit encryption techniques are required. Applications may not store or transmit passwords in clear text.

Any software which stores personally identifying information, including but not limited to, “unique identifier number,” driver’s license numbers, etc., or any financial information, such as credit card numbers, bank routing information, etc., must fully protect the information for the entire duration of the RTRC’s use of the software, as defined in the eventual contract with the successful Contractor, and disclose the methods of protection used, access protection methods, and life cycle handling of this data. Industry standard encryption methods utilizing at least 256-bit encryption techniques are required.

Any HIPAA-related information must be protected in the database and application according to the law (e.g., display only last four digits of the Social Security Number (SSN)).

The Contractor shall supply the RTRC with current HIPAA test results or be willing to be tested with regards to compliance with HIPAA policies on a yearly basis.

11 Database

All database-related components of the solution (e.g. tables, stored procedures, scripts, extensible markup language [XML] schema, and related information) shall be fully accessible and available for support and use by the RTRC and RTRC staff.

Proposer’s solutions should be developed and configured using prescribed standards for SQL Server, and be flexible enough to run in consolidated database environments with other applications using different schemas and virtualization.

Data shall be retained in a read-only historical database for use by management and other RTRC staff to plan and assess system performance, and to address inquiries, conflicts and other related issues.

The system shall allow all such data to be retrieved, even if it has been archived.

All queries made to the database shall be logged for audit purposes. The RTRC shall have the ability to view these logs when required.

The online data storage system shall ensure data integrity in the event of a disk-drive failure.
In addition, the system shall include a means of archiving transaction data, or restoring data from an archive, while the system is in operation. It shall not be necessary to shut down the database to perform a successful backup operation.

Proposers shall determine and describe the need and procedure for an incremental, daily or other time frame-based backup of data. Other needs related to the archiving of data, such as hardware and software, shall also be determined and described by each Proposer.

Data kept for archive purposes must be in location that is still subject to all HIPAA testing and be tested for compliance on a yearly basis.

The system administrator account shall not be used with SQL server applications. If it is, the solution must allow the RTRC staff to change the system administrator password on a periodic basis without limitations.

The Contractor must provide the following:

- Scripts in order to recreate database;
- An entity relationship diagram;
- Database schema with a data dictionary detailing all database entities (e.g., tables, columns, and attributes); and
- Recommended practices document for support and maintenance of the database.

12 General

The system shall allow TCSDS system data to be retrieved, even if it has been archived. In addition, the system shall include a means of archiving transaction data, or restoring data from an archive, while the system is in operation. It shall not be necessary to shut down the database to perform a successful backup operation.

The Proposer shall determine and describe the need and procedures for an incremental, daily or other time frame-based backup of the data (but not less than daily). Other needs related to the archiving of the data shall also be determined and described by the Proposer.

The Contractor must provide the following:

- Scripts in order to create and recreate database schemas, stored procedures;
- Entity relationship diagrams;
- Database schema with a data dictionary detailing all database entities (e.g., tables, columns, and attributes); and
- Documentation of recommended practices for support and maintenance of the database.

13 Data Management

Data shall be retained in a database for use by the RTRC staff to plan and assess operational, financial and system performance, and to address inquiries, conflicts and related issues. Storage capacity must be large enough to retain operational history data for at least two fiscal years.

After two fiscal years, the operational and financial data will be archived in a “non-live” database, and will remain readily accessible when needed.

The Contractor may require the use of State data for development, maintenance, and testing work at an offsite location. ODOT restricts the use of the ODOT network for transmittal of data. However, data may be

---

3 “Non-Live” database refers to a “read-only” database that is not being accessed by any application. This database may not be up and running all the time and can be shut down or restarted, as needed.
transferred using ODOT approved methods, with written approval from the ODOT Information Technology Department. This approval will only be granted upon receipt of a letter certifying the following: the data will be maintained in a secure manner; the data will not be used for any purposes other than those required to fulfill the contract; and upon completion of the project the data will be destroyed. The letter must also disclose the location of the data while under the control of the Contractor. The location is subject to Executive Order 2019-12D (all services must be performed within the United States).

Data backup for both live and non-live databases must be archived at redundant offsite locations.

Proposers must describe the time it would take to restore the data into the database from the backed-up files in the event of a database crash.

The Contractor shall develop a long-term archival plan to store information on optical (e.g., Digital Versatile Discs [DVD]) or magnetic storage (e.g., external hard drives) devices in coordination with the RTRC. This data should be stored in such a way that it is or searchable, and arranged by year so, as it moves beyond the number of years mandated in the RTRC’s document retention policy, it can be permanently destroyed.

The Proposer shall determine and describe in their proposal the need and procedures for an incremental, daily backup of the data. Other needs related to the archiving of the data, such hardware and software, shall also be identified and described by the Proposer.

The Contractor is required to provide a data dictionary. At a minimum, the following must be provided:

- All fields and associated attributes;
- A function within the Admin module to view the data dictionary; and
- Could be used for interface configurations to other applications or Application Programming Interface (API) setup.

14 Data Logging and Retrieval

All incoming and outgoing data shall be stored in a read-only historical database for retrieval, analysis, display and printing.

This historical information shall include all data exchanged between vehicles and dispatch (e.g., location data, vehicle logon/logoff data, device alarms, and canned data messages); and all central software user logons and logoffs.

The stored data shall be time and date stamped, and shall contain sufficient information to enable selective sorting and retrieval based on user-specified selection criteria. At a minimum, the following sorting and selection criteria shall be supported for accessing the historical data from both the online and archived storage: date and time, GPS latitude/longitude, name of service provider, vehicle number, vehicle operator number, dispatcher number, run number, and incident type (where needed).

15 Data Access

The database structures and any proprietary interfaces shall be documented in the proposal. The proposed system shall follow an open architecture model, providing the capability for the RTRC to independently develop system interfaces or enable integration with other internal or third-party systems. The use of standard network communication protocols (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP] and system interfaces (e.g., Open Database Connectivity [ODBC] for databases) is required.
The RTRC shall be allowed royalty-free access to the database tables, and royalty-free use of the
data and interfaces. If necessary, the RTRC shall be allowed to extend such access and use to third
party vendors for integration purposes.
All system data shall be the property of the RTRC and shall be immediately available to the
RTRC. The Contractor shall acknowledge in writing that the RTRC will own any and all data
and the database where the data resides.

16  Customer Support
Customer support shall be available 24 hours a day, 365 days a year. All technical requests from
the RTRC must be addressed within one hour of the notification of a problem. If an issue
requires a longer timeframe for resolution, the RTRC must be advised accordingly and an
expected reasonable timeframe for resolution must be provided.
The RTRC must be able to view the status of their support request(s) at any time through an
online tracking system to be provided by the Contractor.
For on-site support, the proposal shall include a list of the support firms, their support
responsibilities and the response arrangements.
The Contractor shall arrange for support from one or more qualified firms to be available on-site
on a four-hour response basis when needed by the RTRC to assist with fault diagnosis or
component replacement.
If a support firm does not respond within the agreed-to response timeframe, or when a support
firm is not able to provide the needed support, the Contractor shall provide, during the warranty
period, supplementary support in accordance with an agreed-to escalation procedure. The
escalation procedure can initially involve telephone support, but must culminate in the
Contractor providing on-site support, if needed. The proposal must define the proposed support
escalation procedures.

17  Site Installation
The Contractor will provide needed service technicians to assist with installation of product
within the RTRC network. The RTRC will make available, resources to assist with all aspects of
installation with regards to personnel or additional system needs if virtualization approach is
deemed possible. The Contractor will be required to comply with current data center restriction
policies and must be willing to submit to background checks if deemed necessary by the data
center. RTRC personnel will accompany contractor staff at all times during the installation and
may assist as needed.

18  Hosted Approach
Customer support shall be available 24 hours a day, 365 days a year. All technical requests from
the RTRC must be addressed within one hour of the notification of a problem. If an issue
requires a longer timeframe for resolution, the RTRC must be advised accordingly and an
expected timeframe for resolution must be provided.
All servers, routers, switches, data center security and facility power shall be monitored
electronically 24 hours a day, 365 days a year. In the event there are any out of tolerance
conditions with any server components, technical support shall be automatically notified. The
technical support must respond to these issues within one hour of notification.
The data centers to be used for hosting must have existing scheduled routine maintenance and
emergency situation management plans. Proposers must submit maintenance schedules and
emergency plans with proposal for contractor review.
The data centers must comply with all HIPAA requirements as pertains to security and
verification of credentials as well as any access to physical systems containing RTRC data.
Follow-up Analysis
The Contractor shall provide onsite follow-up analysis, including a written report on the findings of this analysis, on how the system is being used and provide training to address the issues. This follow-up analysis shall be conducted every six months under the warranty period and the first visit shall be conducted six months after the system acceptance. The follow-up analysis report shall categorize discovered issues under the following categories:

- Issues due to lack of training;
- Issues that require configuration changes;
- Issues that require system enhancements and can be addressed by upgrading to a more recent version of the system; and
- Issues that require system enhancements and will be fresh development for the Contractor.

Post-Implementation Support and Maintenance Program
ODOT is in the process of developing a Service Level Agreement (SLA) for post-implementation support and maintenance. The Proposer shall provide a sample SLA that addresses these needs.

Software Updates and Upgrades
Proposers must describe their maintenance update and upgrade approaches in their proposals. Proposers shall describe the difference in processes and costs associated with updates and upgrades.

The Contractor is required to notify the RTRC at least one month in advance of the installation when new software releases become available.

The Contractor is required to notify the RTRC at least six months in advance when it is expected that the current releases and related systems will no longer be supported.

The Contractor shall ensure that all existing software configurations are protected after the system has been upgraded or updated for the entire duration of the time when the RTRC uses the product.

The Contractor must comply with the RTRC’s change management process when making any changes to supported systems. These changes must be reported to the RTRC Project Manager.

Wireless Data Communication Requirements

General
The Proposer shall describe the data communication infrastructure required to satisfy the following communication needs for this project:

- Wireless data communication between vehicles located at RTRC agency facilities and the central system; and
- Wireless data communication between the central system and all revenue vehicles throughout the RTRC’s service area.

The Proposer shall identify the specific on-board and central hardware and software that will be required to establish a wireless communication infrastructure.

The Proposer shall identify the necessary cellular data requirements for their proposed solution and include such pricing in the cost proposal using the Price Proposal Form.
23 **Wireless Data Communications**

The Proposer shall provide estimates of the bandwidth required for data exchange between the central system and vehicles (in terms of megabytes [MB] per month per unit). The Contractor shall provide a report to monitor data usage by vehicle on a monthly basis.

24 **Wireless Data Communications Network**

Proposers are required to submit a solution that shall provide data communication as stated in Section 4.1. The solution shall ensure the transfer of data between the central system and each vehicle in the regional transportation service providers’ fleets via a cellular data connection.

The proposed communications protocol shall follow the open system interconnection (OSI) model.

The RTRC will select a cellular data provider in consultation with the Contractor, suitable to support the data communications requirements of the system as best available based on the cellular communications options commercially available to the RTRC.

Proposers shall describe any additional power backup provisions that will be incorporated into the proposed system to maintain operation of the central system, including the cellular data gateway during a power supply failure, and for how long power can be so maintained.

The description of the proposed communication solution shall include at least the following information:

1. Description of the communications protocol to be used (e.g., inter-asterisk exchange [IAX], session initiation protocol, skinny call control protocol [SCCP], and extensible messaging and presence protocol [XMPP]);

2. Description of any data compression and encryption techniques being used for data packets exchanged between regional transportation service providers’ vehicles and the central system. In the event when no encryption is being used, Proposers must clarify the steps taken to ensure data security over the public wireless network; and

3. Information on the bandwidth needed to support the data exchange between vehicles and the central system. Proposers shall assume that location updates shall be provided at an interval of 15 seconds or less from each vehicle. Further, location updates shall be provided at the time of vehicle departure from each pickup and dropoff.

25 **On-Board Hardware**

26 **Data Communication Hardware**

The Contractor shall provide a cellular data modem and other relevant hardware for system data communication needs using a commercial cellular network. The Contractor shall conduct a coverage test, or rely on already available data provided by the RTRC’s IT staff, to determine the carrier with best data coverage in the HSTC Region 9 service area.
27 Antenna Hardware

If applicable, proposed antenna hardware shall help limit the number of antenna hardware to be installed on each vehicle. An antenna which can support a combination of global positioning system (GPS) connection, cellular network connection and wireless fidelity (Wi-Fi) connection using a single unit (e.g., dual-mode antenna, tri-band antenna) may be used for the proposed solution.

The Contractor must use low-profile antenna hardware.

28 On-board Mobile Router Gateway (OMRG)

The modem shall provide a cellular connection over the cellular network to be selected by the RTRC.

The Proposer shall describe the ability of modems and supporting hardware (e.g., network card) to support multiple types of wireless data networks using a single hardware unit (e.g., 4G/3.5G, 3G type cellular data connectivity over a particular carrier network).

The modems shall have the ability to utilize a 4G wireless data connection when such networks are available. The proposed hardware shall be able to automatically switch over to a lower bandwidth network (e.g., from 4G to 3G) in the event a higher bandwidth connectivity is not available.

The hardware may also have the capability to utilize Institute of Electrical and Electronic Engineers (IEEE) 802.11x (commonly known as wireless fidelity [Wi-Fi]) or 802.16x (commonly known as wireless interoperability for microwave access [WiMax]) hotspots where such networks are available.

The modem/router shall support Quality of Service (QoS) in order to ensure protected bandwidth for multiple sub-channels. The CAD/AVL data will need to be guaranteed a QoS to maintain desired throughput for simultaneous transmission of both types of data. The same will be true for video that could be provided by an on-board video surveillance system, which may be procured in the future.

The vehicular modem must be capable of withstanding normal wear and tear, dust and water intrusion, and weather conditions associated with field use inside vehicles.

29 Central Wireless Communication Gateway Software

30 General

A mobile data communications gateway shall be established with the cellular data carrier selected by the RTRC to enable the central system to exchange data messages over the leased cellular accounts with vehicles. The gateway internet connection shall be sufficient to support a data rate that can simultaneously carry all the data traffic for the entire fleet.

The gateway shall have the ability to support multiple wireless networks simultaneously.

The gateway shall be setup in a highly redundant configuration.

The Proposer shall describe the wireless coverage of the proposed cellular carrier. The Proposer’s solution must not depend on a specific cellular carrier.

The Contractor, in coordination with the RTRC’s IT staff, shall arrange for a pool plan with the selected cellular carrier for the regional transportation service providers’ fleets to accommodate all vehicles.
The Proposer shall provide the following information in the proposal in terms of megabytes (MB) per month per unit based on their experience: bandwidth required for data exchange between the central system and vehicles.

The software shall process data messages in the order they are received or based on their associated priorities to be defined by the RTRC.

The RTRC shall provide the required data connectivity and firewall configurations to the cellular data provider.

31 Data Message Processing

The software shall process data messages received from the vehicles, and pass these to the central software.

The software shall process data messages received from the central software and pass these to an individual vehicle or a group of vehicles.

The system shall log relevant details about a data message including but not limited to the following:

- Sender and receiver of a message;
- Type of the message; and
- Follow-up action to a message, if applicable (e.g., acknowledgement).

32 Wireless Local Area Network (WLAN) Data Exchange

33 General

Wireless communication between vehicles and the central system will be provided at regional transportation service providers’ offices using Institute of Electrical and Electronics Engineers (IEEE) 802.11x WiFi hotspots.

The Contractor shall install WLAN access points at a regional transportation service provider’s office to upload and download data when vehicles are within close proximity to the office, as necessary. The Contractor must coordinate with the regional transportation service provider's IT staff for approval of access point locations. The WLAN access points would only be installed if the regional transportation service provider has vehicles that operate service.

The Contractor shall conduct a survey of each regional transportation service provider’s office to determine the number of wireless access points required.

The service set identifier (SSID) for access points shall be not broadcast publicly and must be accessible to only regional transportation service provider’s vehicles. The access points shall avoid significant signal availability outside of the intended coverage area.

WLAN access points shall be installed such that wireless signals are not obstructed by any barrier.

34 Access Point Hardware

The WLAN access points shall support the Wireless Protected Access 2 (WPA2) security standard, or an approved alternate superior security standard ratified by the time of implementation. The RTRC agency shall have the ability to independently change the encryption keys as often as desired.

Each regional transportation service provider shall have the ability to independently adjust the signal strength of each WLAN access point.

Each regional transportation service provider shall approve the specifics of proposed access point locations, signal levels and antenna type/orientations for an acceptable balance between expected
coverage in outlying parts of the intended coverage area and minimizing signal availability outside the facilities. WLAN access points shall meet or exceed the following environmental capabilities:

- Non-operating (storage) temperature: -40 to 185°F (-40 to 85°C);
- Operating temperature: -4 to 131°F (-20 to 55°C); and
- Operating humidity: 5 to 97 percent (non-condensing).

WLAN access points must be National Electrical Manufacturers Association (NEMA) 4 or IP65 rated for dust and water resistance.

35 WLAN Data Transfer Support Software

The WLAN data transfer support software shall manage the WLAN data transfers between vehicles and the central software using the new WLAN at each regional transportation service provider. Wi-Fi hotspots will be required at each regional transportation service provider’s office to upload/download the following information to/from the regional transportation service providers’ vehicles:

- Schedule/manifest data to vehicles; and
- Configurations, firmware upgrades, and patches to vehicles.

Once a vehicle has successfully associated with a WLAN access point, the WLAN data transfer software shall receive the file uploads initiated by the on-board mobile data terminal (MDT). When the WLAN data transfer software has a download available for a vehicle that has successfully associated with a WLAN access point, the WLAN data transfer software shall check with that MDT whether it has already received that download and if not initiate and complete that download.

Any new download file shall be downloaded to the entire fleet within one day, if each vehicle returns to WLAN coverage each night and is configured to remain on for a set time configurable by the regional transportation service provider (e.g., at least 15 minutes after the ignition is turned off).

The system shall report on the status of the current status of downloads (e.g., download in progress, downloaded or download failed) for the regional transportation service provider’s fleet. Updates or changes to schedule data shall be able to be downloaded prior to their effective date for service and then accessed the first time a driver logs on for service for that effective date.

36 GIS and Mapping

37 Map Source

The Proposer shall identify the source of GIS maps data to be used for the proposed TCSDS system. It is assumed that the Contractor will supply the base map, unless the RTRC specifies otherwise. If the base map is supplied by the Contractor, the Contractor is required to provide updates to the map within two weeks from the date when the updates are available. Third-party mapping systems (e.g., ESRI Maps, Google Maps, Bing Maps) may be used as far as they meet the requirements described in this specification.

38 Built-in GIS Support

The software shall incorporate GIS capabilities that allow users to view maps of the service area and individual trip patterns, each at various specified user-defined zoom levels. GIS features
shall be closely integrated with the individual modules of the TCSDS system and access to maps shall be seamless within the TCSDS system modules.

In addition to supporting the primary demand-response service functions, the GIS functionality of the proposed software shall support other GIS analyses and be capable of converting geographic files from other sources (e.g., Tele Atlas or Navteq) to the format used by the Contractor’s GIS (e.g., ESRI).

39  Spatial Layer Management
40  Map Overlay
GIS functionality shall include the ability to develop overlays for the coverage of municipal, township, census tracts or block groups, and zip code boundaries. The system shall allow overlay of terrain, aerial or satellite layers on base maps when such layers are available.

41  Definition and Management of Geographic Boundaries
The system shall allow definition of polygon layers when such layers are not readily available for overlay. The system shall allow the user to assign a specific service characteristic to a polygon layer. These characteristics shall include but are not limited to the following:

- Agency service area for demand response and other services;
- Americans with Disabilities Act (ADA) complementary paratransit service area;
- Town boundaries; and
- Fare zones.

42  Definition of Physical Barriers
The system shall allow the definition or import of physical features that act as barriers to routing (e.g., rivers and lakes, road closures). The system shall recognize these barriers when routing vehicles.

43  Definition of Point of Interest (POI) Locations
The system shall be capable of defining and displaying point files that may represent landmarks, public transit stops, major transfer points, major destinations of travel, or other POI locations (e.g., hospitals/medical centers, assisted living facilities, shopping centers, tourist attractions).

44  Import/Export of Map Layers
The system shall have the ability to import and export map layers in standard geographic file formats (e.g., Environmental Systems Research Institute’s [ESRI’s] SHP file format or Keyhole Markup Language [KML] format). The system shall have the ability to import location data (customer address or POI database) if available in standard "point" file format (SHP or KML) that consist of latitude and longitude data.

45  Management of Spatial Attributes
The system shall allow authorized users to edit the base map layers (e.g., to add new streets, change municipal boundaries, define any incomplete address ranges). A service area map shall include current data for all street segments to ensure, in part, that every segment is appropriately connected in the network and contains the necessary data for scheduling. For each street segment, this data shall include at a minimum a defined street name and address range, and segment speeds by time of day and day of week. The street network definition shall include segment characteristics (e.g., speed limits, one-way direction).
46 Geocoding
The system shall have full geocoding capability, allowing the system to locate the address on the map for an address input. The geocoding capability shall be seamlessly integrated with relevant features in the rest of the TCSDS system (e.g., address input in the Reservations module, discussed later in Section 6.5).
The street segments database shall be sufficiently complete to assure a geocoding success rate of 90 percent or better based on a sample of addresses developed by the RTRC. The system shall be capable of handling various abbreviations of names (e.g. St. for Street and Av. or Ave for Avenue) in the geocoding process.
47 Miscellaneous GIS Features

48 Distance Computation
The system shall allow the user to calculate the distance between points or along a specified portion of the street or road network. The system must be capable of calculating two distances: the least path distance and the actual distance.\(^4\) The system must store both distances so that reports can be run on actual and least-path trip distances. The system shall allow the software user to select the unit of measurement (e.g., feet, mile) when computing distance.

49 Zoom/Pan
The system shall allow software users to zoom in, zoom out and pan map views. The system shall allow software users to zoom in to a street-level view. The system shall allow software users to select custom zoom level (e.g., 400% or 50%). The system shall provide an “inset” view that can be turned on or off by users. The inset view shall display an overview map within the detailed map view and shall allow “pan” capability.

50 Save and Reload Map View
The system shall allow users to bookmark or save a particular view on the screen. The system shall allow users to reload saved map views.

51 Spatial Search
The system shall allow geographic search within TCSDS modules and shall support search based on at least the following data:
- Customer address;
- Trip origin or destination location;
- Current vehicle location; and
- POI location.
The system shall be able to identify whether or not a customer address is located within a buffer zone (e.g., \(\frac{3}{4}\) mile) around a fixed public transit route or within a general public demand response service area. The parameter for the buffer zone shall be configurable. The TCSDS shall allow a user to view a list of all trips to a location or town within a specific time frame. This allows users to see which drivers are already in the area to do non-scheduled trips. This shall be displayed in a map view including real-time vehicle locations and in a table.

52 Legend
The system shall have the ability to display legend of the layers included in the GIS subsystem. The use shall have the ability to turn this feature on or off, as needed.

53 Printing
The system shall be capable of printing maps to peripheral devices (e.g., printers, plotters) directly attached to a workstation or available over a Local Area Network (LAN) or wireless LAN. The system shall allow users to print and save a PDF version of the map view.

The system shall provide users the ability to format the layout of maps before printing. As a minimum the following capabilities shall be available: adjusting margins, adding title, adding legend.

54  **Visualization**
The system shall display vehicle locations on the map when such data is available from vehicles (see Section 9.2.1.3 for AVL tracking).
The vehicle icon on the map view shall display additional information (e.g., operator id, vehicle id) upon user request if such information is available in the system (please see Section 6.10 for MDT interface).
The map view shall support context sensitive menus and shall allow users to communicate with vehicles directly from the map view when such capabilities are implemented by the RTRC (please see data communication requirements in Section 4).

55  **Map Update Process**
The system shall provide the RTRC the capability to update the base map, whether it is supplied by the Contractor or by another source.
Map updates, when available, must be made to the mapping data stored on the RTRC server or hosted system. Map updates should not be performed while a user is accessing the map.
For Contractor provided maps, the RTRC shall be notified in advanced of the map update schedule.

56  **Integration of Real-time Traffic Information**
Integrating real-time traffic information with the mapping/GIS as well as utilizing this information in scheduling and dispatching is required.
The software shall respond automatically to road conditions such as traffic congestion, weather, and vehicle breakdowns by using real-time traffic and mapping information to predict estimated time of arrival (ETA) and estimated time of completion (ETC) for trips within a customer-defined pickup window. The system shall automatically alert dispatchers to any deviations from the schedule and include a method of providing updates to riders via mobile app notifications or automated voice or text messages.
The system shall provide map views to visualize individual, multiple, or all vehicle routes, as selected by the user, that include real-time vehicle location and underlying street map, traffic information, and trip information.

57  **Third-party Mapping (Google Maps, Google Earth, Bing Maps, MapQuest) Overlay/Integration [Optional]**
The system shall have the ability to utilize a third-party GIS subsystem for geographic information display when built-in GIS capabilities are not available. When both capabilities are available in the proposed solution, the Proposers shall provide a comparison of features available in both GIS subsystems in their proposals.
Proposers must describe any user-licensing terms and conditions associated with using third-party mapping products.

58  **Trip Coordination, Scheduling and Dispatching Software (TCSDS)**

59  **Existing Trip and Client Database Conversion**
The Contractor shall be responsible for converting the following databases from the existing software at the agencies that are participating with the RTRC:
• Existing client databases; and
• At a minimum, the most recent year client trip histories.

The Contractor will work with the RTRC Project Manager to develop a list of fields that will be converted from the existing databases to the new database. This development shall include the logic required to populate fields in the new database that have no match in the old databases. In the event that certain fields within the existing client and trip history databases, and associated business logic to derive those fields are not supported in the selected system, the Contractor shall notify the RTRC and negotiations shall be held to determine the importance of the field and whether the RTRC will require customization of the system client database structure to incorporate new fields.

The Proposer must explain how the conversion shall be accomplished.

The proposal shall identify specific quality control procedures to ensure that data is accurately converted and to ensure its integrity.

Prior to performing any data conversion, the Contractor must prepare and deliver a data conversion plan to the RTRC for review and approval.

60 Client Registration

The client database shall include at least the fields shown in Table 3. Specific characteristics associated with the entry of data elements are described after the name of the data field.

Table 4. Required Client Data Fields

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Field Name and Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demographics / Eligibility Determination</td>
<td><strong>Client name.</strong> The system shall require entry of first name, last name, middle initial and suffix (e.g., Sr., Jr., III). When entering data, the system shall detect and alert the user if there may already be a client database entry under this name. Different clients with the same name shall be allowed.</td>
</tr>
<tr>
<td>Demographics / Eligibility Determination</td>
<td><strong>Client’s date of birth.</strong> The system shall require entry of the client date of birth using an interactive calendar interface or drop-down menu, or by entering the date manually. The system shall automatically calculate the client age, expressed in years, based on the current date and the date of birth information.</td>
</tr>
<tr>
<td>Demographics / Eligibility Determination</td>
<td><strong>Client’s gender.</strong> The system shall allow for manual entry or for the field to remain blank.</td>
</tr>
<tr>
<td>Demographics / Eligibility Determination</td>
<td><strong>Client’s eligibility status.</strong> The system shall allow user selection from a pre-defined list of eligibility definitions that include physical and mental disabilities as well as DHHS categories such as protective custody. An “other” category shall be provided to allow manual entry of explanatory notes.</td>
</tr>
<tr>
<td>Demographics / Eligibility Determination</td>
<td><strong>Income data to determine eligibility for low income programs.</strong> Income data is not required. If not provided, the client will not be eligible for certain trips available to low income individuals.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Data Field Name and Requirement</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Address / Phone</td>
<td><strong>Client’s home address.</strong> This text field becomes the default pickup address in the absence of another address that is identified as the default pickup address (see below in Client’s common locations). The system shall allow entry of an address that contains a “½” or “c/o” and shall ensure that the full address is printed on the manifest (e.g., 123 ½ West Market St.).</td>
</tr>
<tr>
<td>Address / Phone</td>
<td><strong>Client’s mailing address if different than the home address.</strong> This text field is used in case the client uses a non-street mailing address. The system shall allow entry of an address that contains a “½” or “c/o” and shall ensure that the full address is printed on the manifest (e.g., 123 ½ West Market St.).</td>
</tr>
<tr>
<td>Address / Phone</td>
<td><strong>Client’s common locations.</strong> The system shall allow multiple address entries for common client pickup locations. If none are entered, the client’s home address shall become the default pickup address. The locations shall be text fields and allow all characters necessary to accurately store and print on the manifest (e.g., 123 ½ West Market St.).</td>
</tr>
<tr>
<td>Address / Phone</td>
<td><strong>Directions to assist in locating pickup address.</strong> The system shall allow entry of a text field for special instructions for subsequent printing on manifests to assist in locating the client address. For example, where it is known that the actual address is different from the geocoded address, this would be noted in this text field for the manifest</td>
</tr>
<tr>
<td>Address / Phone</td>
<td><strong>Client phone numbers.</strong> Multiple fields for home phone, work phone including phone extension, mobile phone and phone number where messages can be left (if different from other phone numbers). The system shall require that one of these numbers is identified as the default client contact phone number. All fields that contain phone numbers shall contain the standard 10 digits for a phone number (xxx-xxxx-xxxx).</td>
</tr>
<tr>
<td>Address / Phone</td>
<td><strong>Backup client contact.</strong> The system shall allow entry of a backup client contact phone number.</td>
</tr>
<tr>
<td>Contacts</td>
<td><strong>Care-giver/emergency contact name, address and phone number to be used in the event of an emergency.</strong> The system shall allow entry of the name, address and phone number of a client’s care-giver/emergency contact.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Data Field Name and Requirement</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Contacts</td>
<td><strong>Caseworker/social worker contact name, address and phone number.</strong> The system shall allow entry of the name, address and phone number of a client’s caseworker/social worker.</td>
</tr>
<tr>
<td>Driver Tier</td>
<td><strong>The driver tier required by the client.</strong> See a definition of driver tiers in Section 6.4.1.</td>
</tr>
<tr>
<td>Vehicle Tier</td>
<td><strong>The vehicle tier required by the client.</strong> See a definition of vehicle tiers in Section 6.4.2.</td>
</tr>
<tr>
<td>Comments / Notes / Special Needs</td>
<td><strong>Client’s mobility aid(s).</strong> The system shall allow entry in a field indicating whether the client uses a mobility aid. The system shall allow selection from among a list of pre-defined mobility aids that includes an “other” category and allows manual entry of explanatory notes. The system shall allow entry of more than one type of mobility-aid.</td>
</tr>
<tr>
<td>Comments / Notes / Special Needs</td>
<td><strong>Disability status.</strong> The system shall require entry in a field specifying disability status. The system shall allow user selection from a pre-defined list of disability definitions that includes an “other” category and allows manual entry of explanatory notes.</td>
</tr>
<tr>
<td>Comments / Notes / Special Needs</td>
<td><strong>Client car seat.</strong> The system shall allow entry in a field indicating whether the client requires a car seat. The system shall allow entry of the type of car seat in a drop down box, with the following options listed: 5 point, High back, Flat and None.</td>
</tr>
<tr>
<td>Comments / Notes / Special Needs</td>
<td><strong>Client mode restriction.</strong> The system shall allow entry in a field indicating if the client is restricted to a particular mode of transportation.</td>
</tr>
<tr>
<td>Comments / Notes / Special Needs</td>
<td><strong>Manifest comments.</strong> This system shall allow entry of comments or information that will appear on all manifest trip entries for that client. The system shall allow a scheduler to view these comments and notes when taking a reservation.</td>
</tr>
<tr>
<td>Comments / Notes / Special Needs</td>
<td><strong>Additional information.</strong> This system shall allow entry of additional information about the client in a text field. Information in this field shall not appear on any manifest trip entry for that client since it may contain HIPAA-sensitive information.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Data Field Name and Requirement</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Funding / Billing</td>
<td><strong>Authorization date.</strong> The system shall allow entry of a date defining when the client is authorized to begin receive service. If this field is left blank the client is authorized to receive service. Since some clients have temporary eligibility, the system shall also allow entry of a certification expiration date. Automatic notifications will be sent to the reservationist or scheduler when authorization will expire within the next week or has expired.</td>
</tr>
<tr>
<td>Funding / Billing</td>
<td><strong>Service suspension date range.</strong> This system shall allow entry of the start and end date for the time period when a client’s ridership privileges are suspended. The system must allow an override of these dates in order to schedule a ride for the client (see Section 6.5.1).</td>
</tr>
<tr>
<td>Funding / Billing</td>
<td><strong>Funding sources/Billing codes.</strong> The system shall allow entry of one or more billing codes for each client, indicating a third party to be billed for certain trip purposes. The system shall allow user selection from a pre-defined list of trip purposes and selection of a billing code for each selected trip purpose. Effective and expiration dates must be capable of being specified separately for specific funding sources. This defines the time period the client is authorized to receive service from a specific funding source. The system shall allow the expiration date to be left blank to indicate the service is ongoing until further notice. Dates shall be entered using an interactive calendar interface or drop-down menu, or entered manually. Also, the system shall allow entry of the limit of the number of units of service allowed per time period (e.g., week, month or year).</td>
</tr>
</tbody>
</table>

The Contractor must provide a portal for funding/purchasing agencies to enter or update client eligibility online. Clients may have multiple eligibilities for various trip purposes. For example, a client may be eligible for Non-Emergency Medical Transportation for some medical trips, while also being eligible for Senior Services transportation for some other types of trips.

The system shall identify and automatically geocode the location associated with each entered address. If the automatic geocoding fails, the system shall provide alternative methods of establishing x- and y- map coordinates for the address. One of the alternative methods supported shall be clicking on a map location with the mouse.

The system shall track the number of trips taken by customers by funding source/billing code and alert the scheduler when the allowed number of trips for a customer for a given timeframe for a specific funding source/billing code has been met (e.g., only ten (10)) trips per customer in a month may be allowed).

The system shall allow software users to attach files to a customer profile in order to store any relevant information. Proposers shall describe the file formats that can be supported in their
The proposed solution. At a minimum, the following formats must be supported: DOC, JPG, PDF, and WAV. The system shall allow the reservationist or scheduler to view these files when taking a reservation.

The system shall allow the RTRC to select specific client information that should be included in the driver manifest.

If necessary, the client record shall be stored with incomplete data. All fields other than last name may be left blank. An alert shall warn the user that there is missing information.

If the proposed system contains additional fields to be considered in client registration, Proposers must include a description of these fields in their proposals.

The system shall assign a unique client identification number for each client entry in the database. The unique client identification number shall be used to link to other tables in the database (scheduled trips, trip history, etc.). The system shall allow a client record to be retrieved by the client identification number.

The system shall allow multiple authorized users to edit customer details in the database at any time.

The system shall keep track of client demographics and maintain a history each time the client details are changed. The RTRC shall rely on this history for audit purposes.

61 Client Data Management

62 Edit Personal Details/Preferences

The system shall allow authorized users to edit customer details in the database at any time.

The system shall keep track of client demographics and maintain a history each time the client details are changed. The RTRC shall rely on this history for audit purposes.

63 Future Tracking of ADA Eligibility by Client

In the future, the system shall be able to track ADA Eligible clients which shall be billed to ADA, based on start and ending eligibility dates and eligibility type.

The system shall automatically suspend standing orders on holidays when TP services are not in operation. The system shall provide a function to allow the reservationist to enter or adjust such holidays. The system shall notify the reservationist upon accessing a client profile within one month of a scheduled trip that a recurring trip will fall on a holiday.

In the future, the system shall track at least the following attributes for each client:

- ADA eligibility start date;
- ADA eligibility end date; and
- Eligibility type such as “Conditional,” “Pending,” “Ineligible,” and “Temporary.”

In the future, the system must alert the scheduler regarding any upcoming expiration dates for client eligibilities.

64 Agency Resource Management

Detailed requirements for managing driver and vehicle information are contained in the following two subsections.

In the future, the Driver Regulations Inventory Vehicle Entry System (DRIVES), which is currently under development, is a comprehensive statewide database of all transportation providers, drivers, and vehicles. While the DRIVES database is separate from the RTRC, the RTRC will eventually need to communicate with it. The RTRC shall have a portal to receive real-time driver and vehicle information. The DRIVES database will track information on driver’s license status and criminal history changes, the vehicle’s registration, the provider’s insurance status, etc.
Driver Management

The system shall provide the ability to manage a list of drivers for each TP that include both agency and volunteer drivers. Because some data, such as driver’s license information, needs to be stored securely, only authorized users shall have access to this part of the system.

The system shall allow the RTRC to specify at least the following attributes for each driver:

- Employment status: whether a driver is employed full time, part time, or volunteer;
- Driver association: whether driver is an employee or a volunteer;
- Employer (TP)
- Date of birth (DOB)
- Driver’s License Number
- Date of hire (hire date for agency drivers and date when a volunteer driver started driving for the regional transportation service provider)
- Employment status: whether a driver is active or inactive (particularly relates to volunteer drivers)
- License information: current status of driver license and type of license (Commercial Driver's License [CDL] or non-CDL), issuing state and license number
- Driver tier (see below for driver tier definitions)
- Medical certifications/licenses (e.g., CPR)
- Status of background checks: date that background checks were performed and due date for the next check
- Date that driver is due for medical exam
- Whether driver has employer-issued cell phone, and if so, the cell phone number
- Whether driver has employer-issued keys
- Volunteer driver schedules: availability and preferences. The system must allow the entry of a permanent schedule (e.g. every Monday, Tuesday and Wednesday) and temporary schedule changes (not available for a range of dates for medical reasons, for example)
- Status of driver training: date that driver received specific training and due date for the next scheduled training
- Whether a safety seat has been issued to the volunteer driver
- Whether volunteer driver has been fingerprinted
- Address: contact address for the driver
- Phone number: primary and alternate contact numbers for the driver

Driver tiers are defined as follows:

- **Tier 1.** Driver may be a provider to independent customers who require minimal customer assistance that can be accommodated in a non-accessible vehicle. Tier 1 drivers do not operate commercial motor vehicles or accessible vehicles. Drivers will not be permitted to provide transportation for passengers who have been identified as unable to self-elect or self-direct transportation services or have a specialized need requiring an accessible vehicle.

- **Tier 2.** Driver may be a provider for Tier 1 and also be a provider to passengers who have a specialized need requiring the driver to provide some level of direct assistance as communicated by the passenger. Assistance may include activities such as assistance boarding or exiting the vehicle, securing a wheelchair, boarding or exiting with other mobility devices, assistance securing seatbelts, or door-to-door service. Driver will not be
providing transportation to passengers who are unable to appropriately communicate their needs to the driver. The driver will be required to meet all Tier 1 and Tier 2 requirements.

- **Tier 3.** Driver may be a provider for Tier 1 and Tier 2, and may also be a provider for passengers with a high level of specialized need that requires the driver to be trained on a wide array of customer service, passenger assistance and sensitivity techniques to serve the specialized needs of passengers. These types of needs may include allowing a passenger to ride without other passengers, assisting the passenger with specialized equipment or communications devices, and assisting the passenger with door through door service, etc. The driver is required to meet all Tier 1, Tier 2 and Tier 3 requirements.

The system shall have the ability to alert the RTRC and employer when a driver’s license renewal, medical exam, or training re-certification is due. The thresholds for alerts shall be configurable.

The system shall allow the RTRC and employer to track volunteer driver details as well as information on the vehicle(s) they drive (see Section 6.4.2). Multiple management and operation reports are based on these data collection fields.

The system shall allow definition of the type of a volunteer driver which could be defined as “personal choice,” “hardship” or “regular” volunteer driver. This field can be left blank.

The system shall be able to track when this volunteer was approved by the employer to provide transportation services to clients.

The system shall provide a view of the unconfirmed volunteer trips for a day, showing pickup and dropoff times and locations, and towns. On the same screen, the system shall display a list of volunteer drivers. Clicking on a driver’s name by the employer shall display their schedule for that day. This allows the employer/TP to easily search driver’s schedules to find a driver that 1) is already going to that town or 2) has the time to do the trip.

The system shall allow software TP users to attach files to a driver profile in order to store any relevant information. Proposers shall describe the file formats that can be supported in their proposed solution. At a minimum, the following formats must be supported: DOC, JPG, PDF, and WAV.

The system shall be able to generate reports on a monthly basis listing volunteers who will have an expired driver’s license or background checks required within a given timeframe.

### 66 Vehicle Management

The system shall provide the ability to manage lists of agency-owned and volunteer-owned vehicles.

The system shall provide the ability to maintain at least the following data about vehicles:

- TP that owns or operates the vehicle
- Vehicle type: agency or volunteer
- Vehicle Identification Number (VIN)
- Make
- Model
- Model year
- Date when vehicle was purchased for TP-owned vehicles
- Vehicle size
- Number of seats
- Wheelchair capacity
- Wheelchair access: lift or ramp
• Fuel type
• Owner (TP or volunteer driver)
• Vehicle tier (see below for vehicle tier definitions)
• Registration status and tag number
• Vehicle insurance information
• Maintenance schedule
• Insurance cards
• Availability status (available, in-service or in-maintenance)
• Date or odometer reading when next service is due for TP-owned vehicles
• Restricted uses
• Other information (e.g., funded by a particular grant or organization, cost broken out by Federal/state/local)

Vehicle tiers are defined as follows:

• **Standard Passenger Vehicle.** A vehicle that is not designed to be handicapped accessible or require a commercial motor vehicle driver license to operate. The vehicle type is similar to those used as a personal or family vehicle and includes: cars, trucks, SUVs or minivans. Tier 1, Tier 2, and Tier 3 drivers can operate a standard passenger vehicle.

• **Enhanced Passenger Vehicle.** A vehicle that has been modified or equipped with features to meet the needs of the passenger with specialized needs other than accommodations for mobility devices (wheelchairs, walkers, canes, etc.). The enhanced passenger vehicle may be equipped with specialized seatbelts, oxygen tank securements, automatic locking doors and windows, entrance steps, defibrillators or other specialized equipment. The vehicle may also be modified in other ways, including removal of seats, addition of a protective shield behind the driver or other modifications to accommodate passengers with specialized needs.

   The specialized passenger vehicle is used to transport passengers with specialized needs, but is not necessarily designed to be accessible for individuals with mobility impairments (i.e., ramp or lift equipped) or require a commercial motor vehicle driver license to operate. Only Tier 3 drivers can operate an enhanced vehicle.

• **Accessible Vehicle.** A vehicle that has been designed to be accessible for passengers with mobility impairments and is equipped with a ramp or lift, but does not require a commercial motor vehicle driver license to operate. An accessible vehicle may be considered an enhanced passenger vehicle when equipped with additional specialized equipment and/or features. Examples of an accessible vehicle are: accessibility equipped mini-vans, accessibility equipped standard vans, and accessible small light transit vehicles designed to seat 15 or fewer passengers. Tier 2 and Tier 3 drivers can operate accessible vehicles with proper licensing as required by state law for operating an ambulette.

• **Commercial Driver’s License (CDL) Passenger Vehicle.** A passenger vehicle designed to carry 16 or more passengers and requires a Commercial Driver’s License to operate. The CDL vehicle may or may not be designed to be handicapped accessible and could have additional features for special service needs. Examples of CDL vehicles include school buses and medium and large transit vehicles, accessible medium and large transit vehicles. Tier 2 and Tier 3 drivers can operate CDL vehicles with proper licensing.
The system shall have the ability to alert appropriate TP and RTRC staff regarding vehicles for which the insurance or registration is about to expire. The thresholds for alerts shall be configurable.

The system shall also be able to track the annual check date for volunteer as well as the volunteer vehicles, insurance and registration Information.

The system shall have the ability to generate a report about TP vehicles for which the registration, safety inspection or insurance will expire in a given time period.

The system shall be able to generate reports on a daily basis, listing vehicles which are due for a state inspection and scheduled preventive maintenance based on mileage and intervals set by the RTRC or TP.

The system shall be able to generate reports on a monthly basis, listing vehicles which are due for inspections or preventive maintenance (including volunteer vehicles).

67 Reservations

Trip reservations can be requested by an individual (the person traveling or a caregiver) or facility (e.g., hospital, sheltered workshop) via a Client Portal or Facility Portal, respectively. Alternatively, an individual or facility can call the RTRC to request a trip.

68 Trip Booking

The system shall permit the RTRC call takers and scheduler to retrieve client records by entering the client ID number, client last name, or other data field such as telephone number. All fields that contain phone numbers shall contain the standard 10 digits for a phone number (xxx-xxxx-xxxx). Once a client is selected, a trip booking data entry screen shall be displayed to the call taker or scheduler pre-populated with all data for that client which remains constant (e.g., ID numbers, mobility limitations). Along with the client data, the system shall display to the reservationist or scheduler all trips booked for a specific client. Also, the system shall allow the reservationist and scheduler to modify and/or cancel any future trips booked for a specific client. The system shall display an alert if a client has already met the quota of trips allotted to them for a given funding source for a given time period, is suspended for traveling during a given time period, or has an excess of no-show trips. The number of no-show trips and time periods shall be defined by each TP.

The system shall also record the name of the person making the reservation; the date and time the caller requested the trip; the number of attendants/escorts; scheduled date of service; requested pickup time; required arrival time at destination; specifics/comments; same information for return trip, if applicable; day(s) of service (if subscription trip); agency billing codes; and required vehicle type, if applicable.

The system shall allow for multiple funding sources to be assigned to a trip. However, the system shall automatically determine funding eligibility and allow the scheduler to change the selected funding source(s) for which the client is eligible.

The system shall automatically present in the trip booking screen the address configured as the default pickup address. The system shall allow entry of an alternative pickup address using keystroke entry or from a list of common locations.

The system shall allow selection of the dropoff address from a list of common locations, including frequently and/or recently used dropoff addresses for that client. The system shall allow entry of an alternative dropoff address using keystroke entry or from a list of common locations.

The system shall provide the ability to book a return trip for a client trip. The system shall include a default pick-up time (configurable by the RTRC) for the return trip, and shall allow the
return pickup time to be left blank if the client will contact the TP when they are ready to be picked up.
The system shall provide the ability to book multi-legged trips by allowing entry of the pickup and dropoff addresses for each leg.
The trip date shall be entered using an interactive calendar interface. The system shall be capable of accepting trip bookings up to 180 days in advance of the requested trip date for subscription trips and 14 days from the requested trip date for regular trips. These thresholds shall be configurable by the RTRC.
The system shall allow entry of a start and end date for the time period when a client’s ridership privileges are suspended. If the selected trip date is within a time period that the client’s services are suspended, the system shall alert the scheduler that the trip booking cannot be completed for this reason. The system must allow the scheduler to override the suspension.
During the trip booking process, the system shall allow entry of the names of any Personal Care Attendants (PCAs) or other companions (e.g., children) that will accompany the client on the trip.
The system shall permit trip booking while the client is on the phone for Open-Door TPs with RTRC-dedicated vehicles. The system shall be capable of booking both subscription (standing-order) and demand response trips in this manner.
For Open-Door TPs with non-dedicated vehicles, the system shall send the trip request to these TPs via a TP Portal according to the information shown in Table 2. TPs shall have the following possible responses to a trip request: accept trip or decline trip. TPs shall not be able to return work that has previously been accepted. Any trip that has not been accepted by at least one Open-Door TP with non-dedicated vehicles via the TP Portal will be removed at a configurable time set by the RTRC and go back into a pool so that the RTRC is aware of them. The RTRC reserves the right to adjust the timeframe that offered trips will remain unaccepted on the TP Portal.
Pick-up time negotiation requirement, if utilized, is no more than one hour before or after the client's desired departure time. The system shall require entry of a requested pickup time and allow entry of a negotiated pickup time within the limits of this window.
The system shall allow the RTRC scheduler to link trips together for a group of two or more individuals traveling to a common destination that will be scheduled, as a matter of system policy, to the same run. The system shall allow the scheduler to remove the link and/or delete the trips.
The system shall allow the RTRC scheduler to designate any completed trip booking as a group booking (e.g., a trip for a group of two or more individuals traveling to a common destination that will be scheduled, as a matter of system policy, to the same run), and then add or delete individual clients from the group booking.
The system shall allow for the identification of service types that are customizable and can be applied at the client level and the trip level. Service types shall include at least door-to-door and curb-to-curb.
The system shall show whether trips that were requested during the previous 48 hours were actually assigned to a driver or vehicle. Further, the system shall show whether trips that were scheduled were scheduled and taken; scheduled and not taken (e.g. cancelled or failure to board); or never scheduled and never taken, with a field for the scheduler to indicate the reason (e.g., no provider available or trip ineligible).
Once all other trip booking information has been entered, the system shall indicate to the RTRC scheduler any applicable fare(s) or co-pay(s) to be paid by the client and any companions. Once data has been entered, the system shall determine the most appropriate trip options for the Open-Door TP with RTRC dedicated vehicles based on client preferences and eligibilities, as stored in the client profile, and the following TP parameters: vehicle tier, driver tier, hours in service and service area/zone. The trip options shall be presented to the RTRC scheduler. The RTRC scheduler shall select one of the options to conclude the trip booking process. The system shall, at the conclusion of the trip booking process, confirm to the RTRC reservationist or scheduler that the booking was successfully entered into the system or sent out to Open-Door TPs with non-dedicated vehicles for acceptance or declination. Also, the system shall present a summary of the booked or offered trip to the RTRC reservationist or scheduler. During each trip booking, the system shall display, using the GIS software capabilities described in Section 5, the map locations for the pickup and dropoff locations. The system shall alert the RTRC call taker or scheduler if the client has previously booked a trip with a trip time period that is in conflict with the selected booking pickup time. The system shall allow the call taker or scheduler to book the trip nonetheless by overriding this feature. The system shall flag all trip bookings for which this override was applied.

In the future, the system shall monitor the percentage of standing order (subscription) trips out of all trips, by hour and day, for ADA-eligible clients, to ensure compliance with ADA regulations (40 CFR Part 37.133(b)).

The system shall be capable of booking same day trips. On the service day, the system shall allow for last-minute changes that modify runs based on last-minute passengers. These changes must be communicated immediately to dispatcher(s) and drivers.

**69 Management of Standing Order (Subscription) Trips for Clients**

The system shall allow the entry of standing order (subscription) trip bookings, with flexible options to specify recurring travel dates. At minimum, the system shall support selection of a recurring daily trip; recurring weekly day or days (e.g., every Tuesday or every Monday through Friday), a recurring monthly day (e.g., every 2nd Wednesday) or a recurring monthly date (e.g., the 4th of every month).

The system shall allow for subscription trips and shall allow the following data to be entered: number of passengers; names of passengers (if necessary); date and time of reservation request; requested days of pickup (by date or day of week); pickup location; destination location; required arrival time at destination; requested pickup time for return trip; specifics/comments; agency billing code; same information for return trip: contact person (making reservation); service type (e.g., door-to-door, curb-to-curb); ability to lock trip out from future reservations; reservationist or scheduler code; required vehicle tier (agency-specific; ambulatory; lift equipped; car seat).

The system shall allow the scheduler to temporarily suspend a particular subscription, with entry of both start and end dates of the suspension time period. These dates shall be entered using an interactive calendar interface or drop-down, or entered manually.

The system shall automatically suspend subscriptions on holidays when provider or agency services are not in operation. The system shall provide a function to allow the entry or adjustment of such holidays. The system shall notify the scheduler upon accessing a client profile within one month of a scheduled recurring trip that will fall on a holiday.

Once all other trip booking information has been entered, the system shall display any applicable fare(s) to be paid by the client and any companions.
Once data has been entered, the system shall display the most appropriate trip options for Open-Door TPs with RTRC-dedicated vehicles based on client eligibilities and restrictions and the following TP parameters: vehicle tier, driver tier, hours in service and service area/zone. The trip options shall be presented to the RTRC scheduler. The RTRC scheduler shall select one of the options to conclude the trip booking process. The system shall confirm that the booking was successfully entered into the system and present a summary of the booked trip.

The system shall alert the user if the client has previously booked a trip with a trip time period that is in conflict with the selected booking pickup time. The system shall allow the user to book the trip nonetheless by overriding this feature. The system shall flag all trip bookings for which this override was applied.

### 70 Trip Modification/Cancellation

The system shall allow the RTRC reservationist or scheduler to access existing trip bookings to edit the pickup address, dropoff address, trip date, and/or pickup time upon client request. The system shall assign a unique identification number to each trip booking record to facilitate trip editing. The unique identification number shall not be automatically reset at any time and must remain unique for a period of at least one year.

The system shall permit cancellation of any trip booking, when consistent with RTRC or TP policies. The system shall retain the trip booking and flag it with the date and time when it was cancelled to facilitate the RTRC’s and TP’s management of its cancellation policies. The system shall track late cancellations and no-shows.

The system shall provide the capability to enter a reason for trip cancellations (e.g., cancellation initiated by client/doctor/caregiver/TP/RTRC, or caused by weather or some other reason). If the cancellation is received after a certain time-window, as defined by the RTRC, it shall be identified as a late cancellation. The system shall allow for recording of whether the ride was taken or if the client failed to board without cancelling the ride.

Any trip modification or cancellation shall generate an audit record – one in which the RTRC reservationist’s or scheduler’s name is noted along with the date and time the change was made, the type of modification that was made, and the reason for the modification (if one is noted).

### 71 Scheduling

At this point, the RTRC will be scheduling trips using the correct driver/vehicle tier on Open-Door TPs with RTRC-dedicated vehicles. Please note that the schedules developed using the process described below shall be optimized in real-time so that the desire to keep RTRC-dedicated vehicles full is fulfilled.

For Open-Door TPs with non-dedicated vehicles, after trips are accepted, the RTRC shall be able to view vehicles on the daily schedule but the non-RTRC activities of the vehicles may not be visible. Open-Door TPs with non-dedicated vehicles shall schedule the accepted trips using their own scheduling systems. Depending on how these trips are scheduled, the trips may or may not be visible to the RTRC.

Closed-Door TPs shall communicate trip schedules to the RTRC via the TP Portal. The RTRC shall authorize funding for these trips.

Closed Door TPs shall be able to create lists of trips that they performed, including subscription trips, in the RTRC TP Portal. The purpose of this functionality is to give the Closed Door TPs a convenient way to create a report of their trips and communicate information about these trips to the RTRC. The RTRC will eventually become the entity responsible for billing funding agencies for the Closed-Door TPs’ trips and paying the TPs for these trips, even though the RTRC did not schedule or broker the trips. This is a way to ensure that the Closed-Door TPs can submit
accurate and legible trip lists that capture all of the data needed by the RTRC for billing. (Please note that the RTRC will not be scheduling these trips.)

Further, this functionality should allow the TPs to easily indicate recurring trips so they do not have to take the time to input the same trip data day after day, week after week, etc. This functionality is intended to offer an alternative to TPs using handwritten lists or self-generated Microsoft Excel spreadsheets to create trip lists that must be emailed, faxed or mailed. The available data fields should be the same as those available in the rest of the software. TPs should have the option of exporting a spreadsheet of these trips in Microsoft Excel for their own records.

The system shall record the dates and user identifiers when trips for Open-Door TPs with RTRC-dedicated vehicles are booked, and trips for Open-Door TPs with non-dedicated vehicles are offered, accepted or declined by TPs and scheduled (or not scheduled).

Optionally, the Contractor shall implement the Transactional Data Specification (TDS) for the purposes of being able to view the trips being performed by the TPs as a result of RTRC trips that are offered and accepted by the TPs. Please note that TDS documentation can be found in Roger Teal, Niels Larsen, David King, Candace Brakewood, Charlotte Frei and David Chia, Development of Transactional Data Specifications for Demand-Responsive Transportation, Transportation Research Board, Transit Cooperative Research Program Research Report 210, Project G-16, ISSN 2572-3782, ISBN 978-0-309-48135-9, © 2020 National Academy of Sciences. Additional materials regarding the standard are available from the National Aging and Disability Transportation Center (NADTC) and AARP. A validator software tool that verifies data messages generated by a software system can be found at https://tcrp.demandtrans.com/.

The system shall allow trips to be scheduled with TP-employed or volunteer drivers.

The system shall be capable of scheduling, in batch mode, all bookings for a future range of dates. Proposers must describe the parameters used in scheduling customer trips. For example, scheduling may be based on the actual street network in the service area, using parameters associated with street network segments as established in the GIS system (e.g., physical barriers, running speed by time of day, and appropriate dwell times for the boarding and alighting of passengers). At least the following parameters shall be included:

- Dwell time;
- On-board capacity;
- Average vehicle speed profile for street segments;
- Grouping based on geographic location of origin and destination of trips;
- Avoidance of street segments with detours/road closures;
- Driver and vehicle tiers; and
- Accessibility needs/mobility aids.

In the future, the system shall permit the RTRC to set priority levels on all ADA complementary paratransit trips, which require higher service standards. Proposers shall describe how the system processes trip priorities during scheduling by the RTRC.

The system shall produce a daily manifest for each run, indicating pull-in and pull-out times, the projected arrival time of a vehicle at each pickup and dropoff location, and listing the trip events in chronological order.

When creating a daily manifest, the system must take into account any vehicle assignment restrictions. For example, certain vehicles can provide only a specific type of trip (e.g., buses with wheelchair ramps).
Once generated, the system shall be able to display all manifests with all driver instructions (for Open-Door TPs with RTRC-dedicated vehicles) for a given day. The system shall provide tools to allow and track manual adjustments to the daily manifests, including manually adding notes and moving trips between manifests. The system shall allow manifests to be viewed on a map using GIS coordinates to display pickup and destination points.

The system shall have internal validation checks to ensure that manifests do not violate work and labor rules (e.g., driver work hours and breaks). The system shall also perform validation checks to ensure that policies limiting travel times for individual passengers are not violated. Validation shall also occur to ensure clients are assigned to the appropriate driver and vehicle tiers.

The system shall allow easy dispatcher entry of trip event completion times (i.e., as written on the manifest by the driver or reported by radio).

The system shall allow subscription run templates to be developed, based on standing orders (subscriptions). The system shall optimize the templates for least distance and/or travel time, based on the street network segment parameters stored in the system.

The system shall schedule each run based on an assigned vehicle, recognizing the accessibility needs of the scheduled clients, client tiers, and vehicle capacity constraints.

The system shall allow trips to be added to an existing run on the same day as the run. The system shall identify and display a range of alternatives for assigning the trip to existing runs for that day so as to best satisfy the requirements of the reservation while minimizing any impact on existing reservations. The system shall present these alternatives in rank order with a numerical “score” to indicate the degree of difference between choices presented to the reservationist or scheduler.

The system shall allow trips to be assigned to a taxi company if no vehicle is available to provide a mandatory trip (such as court ordered visitations or dialysis). The system shall allow for entry of the taxi fare in a trip cost field.

The system shall allow a volunteer driver dispatcher to manually assign trips to volunteer drivers. The system shall present a list of available drivers for a trip, based on their stored schedules. The system shall allow certain trips to be marked priority to indicate a trip where a driver must be found.

The system shall provide a daily view of volunteer trips with no assigned driver, showing pickup time, pickup location and town, dropoff time, and dropoff location and town. At the same time, the system shall present a list of volunteer drivers. Clicking on a volunteer driver’s name shall display their schedule for that day, allowing the user to easily search for a driver that is able to do the trip. The system shall allow the user to easily assign the trip to a selected volunteer driver. The system shall show whether trips that were requested during the previous 48 hours were actually assigned to a driver. Further, the system shall show whether trips that were scheduled were scheduled and taken; scheduled and not taken [e.g. cancelled or failure to board]; or never scheduled and never taken. The scheduler will enter the date and time of the request, and the system shall be capable of producing a report that shows the trip request was then scheduled and assigned to a driver.

### Dispatching

### Trip Management

For Open-Door TPs with RTRC-dedicated vehicles, the system shall allow dispatchers to access run manifests using the run number, vehicle number, client number, or client name. The system shall display the run number, the list of passengers, the scheduled pick up and drop off times for each passenger, funding source for each trip, the scheduled arrival time for each pickup and
dropoff, and any special circumstances. The run manifest display shall list trip events in chronological order, beginning with the next upcoming trip event.
The system shall automatically display any same day manifest changes to the dispatcher, so that the dispatcher can convey these changes to the affected drivers. The system shall allow dispatcher to enter road closure or detour information with respect to a road segment.
The system shall allow the dispatcher to use sorting functions to make changes that improve productivity using manual override, computer assisted, and fully automated modes of trip scheduling. After modifying runs, the system will allow the dispatcher to print each run’s stops and routes in order to have fully updated schedules.
The system shall allow the dispatcher to define a region and display a region’s runs on the computer screen with maps.
The system shall allow dispatchers to process no-shows when reported by drivers. The system shall track any such events.
If a vehicle must be removed from service, the system shall allow the dispatcher to associate a newly assigned vehicle with the run. If no alternative vehicle is available and the run must be cancelled, the system shall attempt to dynamically reschedule all the affected trips onto existing runs, with priority to any trips that were already underway on the affected vehicle.
The system shall allow easy transfer of trip event completion data from a printed manifest (that the driver has used to report trip event data), mobile data terminal or reported by radio/phone. This data must include the trip status (taken, no-show, cancelled), actual arrival time at pickup point, actual time passenger boarded, actual dropoff time, pickup odometer reading, dropoff odometer reading and any notes made by the driver (such as complications with mobility devices or violation of policies [i.e., too many bags]).
The system shall allow dispatchers to add any vehicle event information associated with a trip. The system shall log the information in trip history with corresponding date and timestamp. The dispatcher shall be able to select from a list of pre-configured events or manually enter information.
The following trip data is needed for management information reports: actual arrival time at pickup point; actual time passenger boarded; actual dropoff time; actual odometer reading at beginning of trip (typically at pickup); actual odometer reading at end of trip (typically at dropoff); trip status (taken, no show or cancelled); was trip a subscription trip; trip number assigned; total vehicle and revenue miles for each vehicle; total vehicle and revenue hours for each vehicle; and any additional information required (manual entry).

74 Incident Management
The system shall allow the dispatcher to initiate a new incident report. The new incident report form shall appear in a separate window, including an automatically generated date/time and a list of incident types.
The dispatcher shall be able to select an event to form the basis for an incident report, with the incident report form auto-populated with all information already known in the system about the event.
There shall be one central incident/accident report accessible from a server so everyone sees the same current report information, but only one instance of the report can be open at a time for editing.
The system shall allow authorized users to append to an existing open incident report, with other system users limited to read-only access.
The system shall allow authorized users to view and append to an existing open incident report, with other system users limited to read-only access. The user shall be able to select from a list of currently open incident reports that can be sorted by date/time, incident type or initiating dispatcher. The selected incident report shall appear in a separate window, and shall be available for editing.

The open incident report shall be repeatedly accessed and modified, until it is marked closed after which further modifications shall not be possible, unless by authorized personnel with specific authorization to do so.

The system shall allow authorized users to close an existing open incident report. The user shall be able to select from a list of currently open incident reports, which can be sorted by date/time, incident type or initiating dispatcher. The user shall be asked to confirm the selected incident report before the incident is closed.

The incident report database shall indicate for each incident report the date/time of opening the report, the incident type, the initial incident text, the initiating user, the date/time of each subsequent modification, each modified version of the text, the modifying user(s), the date/time the incident was closed and the closing user.

Authorized users shall have the ability to attach files (e.g. an image file) to the incident report. The system shall track the user and date/time when the incident report is opened, modified or closed.

75  Billing and Reporting
In order to enable the system to bill funding agencies, the system must be able to track, for both Open-Door and Closed-Door TPs, the number of trips, number of miles, tolls paid by drivers and trip status (trip taken, no-show, cancelled) by client for each funding source.

The system must provide a mechanism for TPs to bill/invoice the RTRC.

Closed-Door TPs shall invoice the RTRC for the service they provided by uploading the invoice via the TP portal.

Closed-Door TPs shall submit service data reports about provided trips to the RTRC using a form in the software.

The Billing module shall allow the RTRC to define and customize the following information to implement and track multiple billing rules based on the terms of negotiated contractual agreements, and/or grant agreements. The system shall allow the RTRC the option of tracking this data by contract year, RTRC’s fiscal year or other date range (e.g., year-to-date, quarterly).
76 Funding Sources
The system shall be able to track as many funding sources as necessary. The system shall allow definition of at least the following attributes related to funding sources:
- Unique system-generated identifier by funding source;
- Funding source name;
- Funding source address;
- Contract effective and expiration dates;
- Maximum contract dollar amount for the contract time period; and
- Funding source status to indicate whether funding source is currently active or whether it is used for historical or future trips.

77 Billing Rates
The system shall be able to track multiple billing rates for each funding source. Per trip, per passenger-mile, per least path distance passenger-mile, per-revenue mile, per-total mile, per-revenue hour, and per-total hour rates shall be entered for each TP. Rates may be able to be left blank. The system shall allow rate changes any time a new rate is put into effect. The old rate’s expiration date should be updated and the new rate added with a new effective date. Billing charges shall be calculated for each trip date using the billing rates applicable for that date. Trip status must be taken into account when determining which trips to bill. For example, not all funding sources will pay for no-show trips. Trips are charged at different rates based on trip mode category and include trip charge, mileage, tolls and taxi fares. The system shall allow and track the collection of donations (not fares) for trips billed to other funding sources. Please note that for shared rides, the RTRC should be able to allocate shared ride trip data so that it is possible to bill the proportionate costs of shared rides to the appropriate funding agencies based on all possible rate structures (e.g., per-mile or per-trip).

In the future, the TPs must be able to communicate TP rates from a future web-based rate-setting tool. Information regarding the Mobility Ohio Pilot Rate-Setting Tool can be found in https://www.transportation.ohio.gov/wps/portal/gov/odot/programs/transit/transit-coordination-resources/mobility-ohio.

78 Fiscal Years
The system shall account for and manage each funding source’s fiscal year date range.

79 Trip Mode Categories
The system shall be able to track multiple trip mode categories. Trip mode is a mandatory field in all billing and reporting options. The system shall be able to track multiple trip mode descriptions such as “Van,” “Bus,” “Taxi,” “Self Transport” and “Volunteer.” The system shall be able to track and implement rules which require specific codes for modes of transportation and HIPAA related codes, as well as reimbursement rates.

80 Trip Purpose Categories
The system shall allow the RTRC to track multiple trip purpose categories based on specific billing source contractual agreements and billing rules. Some funding programs may define specific trip purpose categories which are correlated to eligibility, billing and reporting options.

81 Driver Details Tracking
The system shall allow tracking of pre-and post-inspection times for agency drivers.
82 **Trip Status Categories**  
The system shall allow the RTRC to customize and track as many trips statuses as necessary. Based on contractual agreements, only certain trip statuses may be billed. For example, No-Shows may have different billing rules under different funding programs. All reporting options shall use the trip status field in the criteria selection and sorting. The system shall allow the RTRC to update status of a trip such as “scheduled taken,” “denied,” “cancelled by client,” “cancelled by office,” “late cancel,” “no-show,” “driver no-show” or “inability to find driver.”

83 **Billing Status Categories**  
The system shall allow the RTRC to customize and track as many billing status categories as necessary.

84 **HIPAA Transportation and Other Codes**  
The system shall be able to track HIPAA compliant transportation and other service related codes by TP.

85 **Trip Details by Client**  
The system shall be able to track multiple rides per client, using the unique client identification number as described in Section 6.2. This assumption is being used when defining specifications for tracking individual client trip details and billing options. The system shall allow entry of the following information for billing with respect to the client trip data entered in the system as part of trip booking process (see Section 6.5.1)

- Funding Source Identification: to track the trip Funding Source ID
- Vendor ID: to track the PT’s Vendor ID
- Mileage: used in all billing, management and operations processes and reports to track mileage statistics.
- Trip Charge: used in all billing, management, operations and associated processes to track trip charges per trip.
- Other charges: to track other charges when clients incur expenses for other services that are related to transportation needs, such as hotels, meals, tolls, parking fees. Rules need to identify and process such charges differently. These charges are not included in reporting and analysis options which summarize regular trip charges.
- Fare or Co-Pay Amount: to track and look up fare amounts per trip. Cross Reference to Fare or Co-Pay Amounts by Billing Source specifications. The Contractor shall be given the fare matrix that will be necessary to look up fare amounts per trip.
- Invoice Date: to track when Invoices are balanced and generated.
- Billing Status: to track multiple billing statuses
- Resubmit Flag: A “Resubmit” is a trip record which was denied and needs to be billed again, after errors in processing are fixed. Resubmitted trips cannot be double counted, while reconciling and generating statistical agency wide reports.

86 **Other Contracts**  
The system must be able to generate billing reports/invoices for local partners, state agencies and third parties (e.g. other contracts).
The system shall be able to generate billing reports for internal accounting and specific contract required billing procedures that list clients, trips, time, mileage, and other parameters for a given time period.

87 Fares
The system shall be able to generate a report of daily fares, co-pays and donations broken down by run.

88 Customer Service
The system shall allow customers to fill out a brief survey after their trip to indicate satisfaction with their ride/the service. This feedback shall be logged along with any responses made as a result of the customer feedback. The survey shall include the opportunity for the customer to input an open-ended comment and a rating for the trip, in addition to yes/no or multiple-choice questions.

The system shall have the ability to log and track the status of customer complaints and commendations.

The system shall automatically assign an identification number or a case number once the complaint or commendation is saved.

The system shall allow the input of at least the following information with respect to a complaint or commendation:
- Client identification number (when the customer is not registered, allow for information to be ignored or for passenger name to be entered instead);
- Reason for complaint (e.g., later arrival of vehicle) or commendation;
- Billing source;
- TP name
- Date and time of complaint or commendation;
- Current status of a complaint or commendation;
- Current owner of the case (who is handling the complaint or commendation currently); and
- Ability to generate a report showing complaints and commendations for the month by program/billing source.

The complaints/commendation module shall support workflow management which shall allow agency staff members to assign a case to a specific agency employee’s queue (currently only one person handles complaints/commendations) depending on the nature of the complaint or commendation.

The system shall have the ability to alert the authorized management staff automatically about any complaints or commendations that have not been addressed for a defined period of time and closed out.

All data shall be stored in the TCSDS database and the RTRC shall have ability to run reports that require access to this data.

89 Mobile Data Terminal (MDT) Interface
Requirements in this section assume that TP vehicles shall be equipped with MDTs and data modems. On-board equipment is described in Section 9.2.1.

90 Data Messaging
The system shall allow the dispatcher to view received text messages in a tabular display that also indicates the vehicle ID and the time of the message.
The system shall allow the dispatcher to send a text message to a single MDT, a predefined group of MDTs or all MDTs within an area selected on the map display.

The system shall allow the dispatcher to select one of a set of predefined text messages or enter a free text message.

The system shall allow any message sent by dispatch to be flagged as requiring operator acknowledgement, and shall allow the dispatcher to view a list of such messages that have not yet been acknowledged.

91 Manifest Transmission and Changes
The system shall produce a daily manifest for each run, indicating pull-in and pull-out times, the projected arrival time of the vehicle at each pickup and dropoff location, listing the trip events in chronological order.
The system shall be able to generate and display all manifests for a given day. The system shall provide tools to allow manual adjustments to the run manifests, including manually moving trips between manifests.
The system shall send manifest trip pickup and dropoff data to the MDT in the vehicle assigned to that manifest.
The system shall send the manifest for the next day to each driver via e-mail.
The dispatcher shall be able to configure which portions of the upcoming manifest entries shall be sent to the MDT (e.g., the next X trips, all trips in the next Y minutes).
Additional portions of the manifest shall be automatically sent to the MDT on an ongoing basis as trip events are completed, in accordance with RTRC-configured manifest transmission parameters.
The system shall automatically display any same day manifest changes, such as trip additions, no shows or cancellations, to the dispatcher and transmit these manifest changes to the MDT in the vehicle assigned to that manifest, displayed in a different color text or highlighted.

92 Trip Events Logging
The system shall receive trip pull-in, pull-out, pickup, no-show approval requests and dropoff event reports from MDTs, and use this data to update the time and reported location for each trip event.
The system shall acknowledge the receipt of trip event messages to the MDT.
The system shall store trip event messages sent to the MDT and acknowledged by the vehicle operator.
Based on the logged trip events, the system shall update the estimated time of arrival for the remaining manifest trips and display this information to the dispatcher. This does not change the actual manifest – this updated information informs the scheduler/dispatcher so that they can inform clients if their pickups are expected to be delayed.
The system shall receive no-show approval requests from MDTs, allow dispatchers to decide whether to authorize the no-show, record the time when the no-show was authorized, mark the pickup and dropoff in the manifest as a no show, and transmit the cancellation of the pickup and dropoff as manifest changes to the MDT in the vehicle assigned to that manifest.

93 Passenger Signature for Medicaid Trips
For Medicaid trips, the passenger and driver must sign the manifest to attest that the RTRC has provided the trip. A record containing the two signatures, driver’s license number, vehicle
number, and license plate number must be generated for use when Medicaid trips are processed for payment.

94 Customer/Rider System Requirements

95 General
The system shall allow riders to select and update primary and secondary preferred communication channels, and shall automatically distribute all communications via both preferred channels.

96 Self-Service Communication Channels
The system shall provide at least the following self-service options and communication channels to riders or integrate with currently available customer technologies to provide such self-service options and communication channels:

- RTRC phone system;
- IVR system as described in Section 9.3.4;
- Short message service (SMS) text message as described in Section 9.3.3;
- Email, as described in Section 9.3.3;
- Web Portal provided by the successful Proposer as described in Section 6.5; and
- Mobile application provided by the successful Proposer.

The system shall allow customers/clients or their designated caregivers or service providers to access their trip history (including ability to define a history over a user-defined date range), scheduled trip information, customer/client profile, and account balance via all self-service channels.

The system shall allow riders to access all information about a trip’s status during the day of service via all self-service channels.

The system shall allow customers/clients to schedule, modify, cancel, and track trips within customer policy and procedure limitations set by the RTRC, via all self-service channels.

The system shall allow customers/clients or their designated caregivers or service providers to update their rider account profile via all self-service channels.

The system shall send customers/clients or their designated caregivers or service providers a trip rating message via the rider’s preferred communication channels at the end of each trip and record the rider response as a part of the trip’s record (as described in Section 6.9).

The system shall provide the ability to solicit feedback through surveys at the completion of each trip for a randomly selected rider sample and record the feedback as a part of the trip’s record.

97 Eligibility-Related Communications
The system shall communicate key eligibility information with customers/clients or their designated caregivers or service providers, including appointments and eligibility changes (e.g., eligibility appointments, reevaluation assessment, suspensions, expiration) according to customer policies and procedures.

98 Night Prior Reservation Confirmation
The system shall send out reservation confirmations based on the customer/client’s preferred method of communication to inform riders of the next day’s scheduled trips.

The system shall communicate to with customers/clients or their designated caregivers or service providers the details for each trip including date, pick-up window or the actual pickup time,
origin and destination, and fare. The number of communications sent to each customer/client will be based on the number of trip reservations (i.e., a round-trip made as a single reservation will receive one (1) message).

The system shall attempt to contact with customers/clients or their designated caregivers or service providers through alternate communication channels if the initial communication attempt is unsuccessful (i.e., message undeliverable; call not answered and voicemail left) through the rider’s preferred channel. Customer/client shall define the number of unsuccessful attempts prior to trying a different channel.

The system shall complete all reservation confirmations by a customer-defined time on the night prior to the scheduled trips.

99 Day-Of-Trip Update

The system shall automatically send trip alerts to customers/clients related to any changes that may impact the scheduled pick-up window (e.g., vehicle break-down).

The system shall communicate to with customers/clients or their designated caregivers or service providers the details for each trip, including the origin and destination of the trip, the actual pickup time, and the estimated time of arrival (ETA) in real-time based on actual conditions in any instance where the scheduled trip details have changed.

100 Trip Status

The system shall automatically push trip status updates to customers/clients or their designated caregivers or service providers based on pre-determined parameters (e.g., arrival time, vehicle location). The system shall also allow customers/clients to customize trip status preferences and access trip status and information on-demand. Trip status updates shall include the following information:

- Date;
- Pick-up window or actual pick-up time;
- Origin and destination;
- Fare or co-pay if required;
- ETA in real-time based on actual conditions; and
- Actual vehicle location for trips within thirty (30) minutes of the pick-up window or actual pick-up time.

Within a customer-defined actual pick-up window, the system shall provide customers/clients with access to real-time vehicle location information and estimated time of arrival with the ability to monitor vehicle location through actual pick-up.

101 Cancellations

The system shall communicate to customers/clients the details for the trips that they request to be cancelled prior to cancellation to ensure the proper trip is cancelled. Trip details to be communicated prior to effectuating any cancellation request include: date, pick-up window or the actual pickup time, and the origin and destination.

The system shall notify customers/clients if cancellation is in violation of customer policy and/or carries a penalty.

The system shall request, but not require, riders indicate the main reason for cancellation based on customer-defined fields.

The system shall provide the customers/clients confirmation that the trip has been cancelled via the customer/client’s preferred communication channel.
102 Rider and Account Information
The system shall allow customers/clients or their designated caregivers or service providers to modify the following account information as needed:
• Favorite addresses (e.g., home, work);
• Phone number;
• Primary contact;
• Secondary contact;
• Password;
• Security questions;
• Language preference;
• Preferred communication channel;
• Emergency contact;
• E-mail address; and
• Payment Information if applicable (via connection to customer’s payment system; no payment data will be stored in the rider database within the system or otherwise accessed or stored by vendor).

The system shall allow riders to view, but not modify, eligibility end date and will automatically notify riders via the rider’s preferred communication method when the rider must have eligibility reviewed.

103 Reports
The reporting system must first present data in a summary format and then allow users to drill-down and drill-through the tables for further details. Any graphical illustrations shall be provided as necessary.
Reporting is required for both internal and external use.
The system must allow sorting, grouping and filtering of information on-the-fly by relevant data fields.
The system must allow the RTRC to export all trip data into a spreadsheet to perform analysis.
In addition to canned reports required in the system, the reporting tool must allow the RTRC to generate and save ad-hoc reports easily.
The system shall allow reports to be viewed on screen, sent to a printer or saved to a file.
The system shall allow the RTRC to access the database to create and execute stored procedures written by the RTRC.
The software shall provide standard reports based on the stored data. Proposers shall provide details in their proposal related to reports that are offered and degree to which they can be configured. The standard reports shall include at least reporting on:
• Logon/Logoff summary
• Trips provided
• Non-revenue vehicle hours and miles (the time from when the vehicle leaves the garage to the vehicle’s first pickup, driver’s lunch time, time from the last drop-off to when the vehicle is fueled and brought back to the garage)
• Passenger travel time, by run or user group
• Revenue vehicle hours and miles (hours of vehicle operation in which there is the expectation to carry passengers)
• Passenger-miles, by run or user group
• Least path distance passenger-miles, by run or user group
• Number of cancellations
• Number of no-shows
• Data specific to shared rides depicting the proportionate time, mileage, and costs of shared rides distributed among appropriate funding agencies based on various possible rate structures (e.g., per-mile or per-trip).

It is critical that the software provides the RTRC the ability to access data to assist in the analysis of passenger trips, vehicle miles, and vehicle hours whose costs are shared by multiple funders. Growth in cost-efficiency through shared rides and braided funding is a critical performance measure for the Mobility Ohio pilot project. See Figure 3 for an illustration of a demand response vehicle run with rides that are shared between clients of multiple funding agencies. The RTRC should be able to use the software to determine passenger-miles, vehicle miles, vehicle hours, and costs associated with each funder (e.g., from Figure 4 example: Medicaid, Senior Center, and Other).

The software shall have the capability to generate reports based on exceptions as per thresholds set by the RTRC.
If reporting shall be provided via a third-party application (e.g., Crystal, Jasper, Power BI), that application must be identified in the Proposer’s response.
In the future, the RTRC shall define the need and elements required for a dashboard for system users. The Proposer shall describe their capability to build a dashboard that can provide access to reporting as well as operational performance metrics.

Figure 4: Demand Response Route with Shared Rides

The software shall have the capability to generate reports based on exceptions as per thresholds set by the RTRC.
If reporting shall be provided via a third-party application (e.g., Crystal, Jasper, Power BI), that application must be identified in the Proposer’s response.
In the future, the RTRC shall define the need and elements required for a dashboard for system users. The Proposer shall describe their capability to build a dashboard that can provide access to reporting as well as operational performance metrics.
104 Computer-aided Dispatch (CAD)/Automatic Vehicle Location (AVL) Functional Specifications

105 General

106 Environment

Equipment modules, cables, mounting hardware and connectors shall be designed to withstand the full range of operating environments found in the areas in which they are to be installed, and shall not interfere with the operation of existing onboard equipment.

Equipment shall operate in accordance with these specifications for ambient temperatures from -22 °F (-30°C) to 140 °F (+60°C). If not compliant, please provide operating temperature ratings for the equipment.

Equipment shall withstand without damage being stored for extended periods in ambient temperatures from -40°F (-40°C) to 158°F (+70°C). If not compliant, please provide storage temperature ratings for the equipment.

Equipment shall operate in accordance with these specifications for ambient humidity from 5% to 97%, non-condensing. If not compliant, please provide humidity ratings for the equipment.

Equipment shall be sealed against dust and water intrusion, certified in compliance with or exceeding the National Electrical Manufacturers Association 4 (NEMA4) or International Protection 65 (IP65) standard.

Equipment shall conform to the Federal Communications Commission (FCC) Part 15 Class A limits for conducted and radiated emissions of electromagnetic interference and radio frequency interference.

Equipment shall be tested and proven capable of withstanding power transients, electromagnetic interference and radio frequency interference without degradation at levels encountered in typical transit and paratransit operations.

Onboard equipment shall be specifically designed for the harsh transit environment and shall meet the requirements of this specification under all conditions encountered in typical transit operations.

Onboard equipment provided shall operate in accordance with these specifications while withstanding the vibration and shock forces encountered in typical transit operations.

Cabling and wiring shall be installed in accordance with these specifications while withstanding the vibration and shock forces encountered in typical transit operations.

107 Installation

Proposers shall describe (through text, drawings or illustrations) the mounting mechanism by which the tablets will be installed in TP vehicles. The proposed mount design shall account for the safety, performance, ergonomics and usability of the tablet by TP staff. The mount shall have a locking mechanism to prevent theft or vandalism of the tablet.

The tablet mount shall comply with US heavy duty vehicle Society of Automotive Engineers (SAE) J1455 standard. Proposers are encouraged to provide crash and vibration testing ratings of the proposed mounting mechanism.

The installed location of onboard components shall be determined in collaboration with the TPs. The Contractor shall submit Installation Design Documentation (IDD), for TP approval prior to undertaking any installations.
The IDD shall provide text, drawings, illustrations and images using adequate detail to allow for quality installation by a technician without further training in conjunction with other installation instructions provided by the vendors of individual equipment components.

The IDD shall include details on (1) equipment installation locations/mounting; (2) routing, conductors, color-coding, labeling, and connectors for power, communications and vehicle ground circuits; (3) connections with, any required modifications to and restoration of existing infrastructure; (4) work area and equipment storage requirements; (5) methods and quality standards; and (6) supervision and quality assurance procedures.

The IDD shall include procedures for pre- and post-installation checklists for tests to be performed by installers. The installations shall not be considered complete unless the TP provides signoff on the pre and post installation checklist for each vehicle.

Equipment shall be properly grounded, with onboard equipment connected as directly as possible to the chassis ground.

Equipment components shall be replaceable as discrete units and identified by unique serial numbers. Each connector shall be keyed or otherwise configured so as to prevent inadvertent mis-wiring during MDT replacement.

Equipment inputs and outputs shall be protected, to absorb “routine” electrostatic discharges, over-voltages and reverse polarity conditions. In the event of “extraordinary” conditions, equipment shall be designed to sacrifice inexpensive and easily identifiable components when necessary to protect more expensive components or those less easy to troubleshoot.

Equipment shall be housed in enclosures that cannot be opened with standard hand tools, and resist damage from vandalism.

Onboard equipment shall operate from the vehicle electrical system, between 9 and 35 volts. Onboard equipment shall be securely mounted in the interior of the vehicle, clear of obstructions and interference-generating devices, and so as to avoid blocking vehicle operator sightlines to front and side windows.

The MDT shall be mounted within comfortable reach of the controls from the seated position for the full range of vehicle operators and vehicle types.

The installed location and mounting method for the MDTs shall be determined in collaboration with the TPs’ staff. If deemed necessary by a TP, the Contractor shall rearrange the installed locations of other onboard equipment to achieve a suitable overall arrangement of equipment (e.g., radio/handset).

Installations shall be performed at specific times during the day and as approved by each TP. The Contractor may be required to perform installations over nights and weekends, and installations may need to be performed at the vehicle’s home base.

Each TP reserves the right to limit no more than 5% of its vehicle fleet to be out of service within any given 24-hour period to accommodate vehicle installations. Each TP reserves the right to allow less of its vehicle fleet to be out of service if necessary in order to avoid disruption to revenue service in conjunction with maintenance requirements.

The Contractor shall ensure that all vehicles made available for overnight installation work are ready for revenue service by the start of the next service day.

The Contractor shall install and configure the entire system, including any TP-provided computer hardware and integration with existing systems.

The Contractor shall provide all necessary personnel, tools, test equipment, transportation, hardware and supplies for the successful and complete installation of all equipment and software.

The Contractor shall be responsible for their own and subcontractors' performance and safety.
Installations shall be performed in accordance with all Federal, State, and local laws and regulations.
The Contractor shall supply any electrical equipment necessary to operate system components using existing DC electrical power available on TP vehicles and existing AC electrical power at TP garages/facilities. If existing power arrangements are unsatisfactory, the Contractor must specify proposed alterations.
The capabilities of existing infrastructure affected by or to be integrated into the new system, such as the TPs’ local area network(s) (LAN) and wide area network(s) (WAN) shall not be reduced at any time by system implementation.
The Contractor shall only be authorized to undertake installations after each TP approves of a pre-installation inspection for each installation site, documenting the existing condition of any existing infrastructure that may be affected by the installation.
Depending on installation needs, installations may be performed at each TP’s garage/facility. Each TP shall be in-charge of removing and recycling any existing TP equipment replaced by equipment provided by the Contractor.
After installations, the Contractor shall be responsible for restoring the condition of any affected existing infrastructure at the installation site to its pre-installation condition.
The Contractor shall be responsible for the security of equipment prior to installation.

108 TP Responsibilities
Each TP will provide space for the Contractor to establish secure storage facilities adjacent to each installation area. The Contractor shall provide details on the space required for equipment storage and vehicle installation.
Each TP will provide space for central system installations and vehicle installations.
Each TP will provide light and electrical service at the installation location, as well as access to compressed air at vehicle installation locations.
Each TP will provide staff to move vehicles to and from the installation locations.

109 On-board Systems

110 Mobile Data Terminal (MDT)

111 General

The system shall incorporate a portable and standalone, tablet-based mobile data terminal (MDT) that can be easily transferred between vehicles and sites. In consultation with the Contractor, TPs will select and may furnish the tablets (rather than being furnished by the Contractor) which will serve as the vehicle-operator interface and MDT. Proposers shall recommend commercial off-the-shelf (COTS) hardware that can meet the requirements herein given their proposed software solutions.
The vehicle operator terminal shall be connected with or integrated into a Vehicle Logic Unit (VLU), and the combination will be subsequently referred to as the MDT. ODOT is considering an MDT to be a tablet that TPs may be able to procure from sources other than the Contractor.
MDTs shall turn on automatically when the vehicle power is turned on, and shall shut down at an agency-configurable time after the vehicle power is turned off. The system shall have built-in battery backup to compensate for any loss of power draw from the vehicle battery when the vehicle is not running.
The MDTs, which serve as the controlling computing device, shall be capable of being locally and remotely configured, diagnosed and maintained. The local configurations shall use a laptop computer or other portable programming device (e.g., via a universal serial bus [USB] port, RS-
The local configuration shall be accessible to the units and shall not require excessive customization between vehicle types (i.e., an identical location and connection shall be used for each type of vehicle).

The Proposer shall provide details on its capability to remotely configure and reset MDTs. The MDT shall be equipped with a navigation assistance module to provide visual and audible turn-by-turn instructions with real-time traffic information for operators of revenue vehicles.

### Vehicle Operator Display

The operator terminal of the MDT shall use a color backlit display, readable by the vehicle operator from the seated position under the full range of ambient illumination conditions. This includes capabilities such as vehicle operator-controlled brightness/contrast control, anti-glare coating, and adjustable orientation mounting.

The color combination to be used on the MDT terminal shall provide legibility for the color blind.

The operator terminal shall be operated using either at least eight programmable function keys with tactile and audible feedback or touch screen programmable buttons with visual and audible feedback.

The MDT speaker shall provide audible feedback when a function key or on-screen key is pressed.

The operator shall not be able to manually shut off or disconnect the operator terminal power or manually shut down the MDT application software.

### “Safe Driving” Mode

For driver safety, the MDT shall have the “safe driving” mode enabled when the vehicle is moving above a configurable speed limit (e.g., 5 miles/hour).

The safe driving mode shall allow TP management to determine the criteria that will prevent vehicle operators from interacting with MDTs when driving. The MDT shall allow the TP to enable the following screen configurations under safe driving mode:

- Blank display on the screen;
- Disabled MDT buttons to stop vehicle operators from performing any actions on the screen; and
- Display of information relevant to vehicle operators when of high priority (e.g., navigation, manifest, or missed messages or calls from dispatchers).

Each TP shall have the ability to remotely change the configurations for the safe driving mode. Each TP shall be able to change the safe driving mode configurations by vehicle operator login. For example, the safe driving mode could be disabled for maintenance or training purposes.

### Navigation Assistance

The MDT shall be equipped with a navigation assistance module to provide visual and audible turn-by-turn instructions with real-time traffic information to vehicle operators.

The MDT shall display a map showing the current location of the vehicle, the location of the next pickup or dropoff, and a continuously updated suggested routing between them, at the
closest zoom level where this route fits on the display. As the vehicle travels, the map view will automatically pan and zoom to continue to show this entire routing at the closest possible zoom level.

The MDT shall allow operators to override the map zoom level or pan the map display, and to select for the display to return to the default mode that automatically follows the routing. The driving instructions shall include both the turn directions and the name of the street, and this information shall be provided at a TP-configurable distance in advance of the turn. The navigation module shall allow the operator to activate and deactivate the navigation map display and/or the audible instructions as desired.

The navigation map shall be updateable over the bulk data transfer using the WLAN or other means.

If the navigation application is active when a manifest change notification or text message is received, the audible alert tone shall be provided without interrupting the navigation application. This will allow the operator to acknowledge and review the manifest changes or text messages at the next appropriate opportunity without interrupting the navigation support.

The navigation assistance system shall not direct vehicles operators to streets that have restrictions for their vehicles (e.g., restrictions on bridge clearance for oversized vehicles).

115 Vehicle Operator Logon

The MDT shall allow vehicle operator logon using operator ID and run ID entry. The MDT shall check with the central system to validate that the operator ID and run ID are valid (and not already logged in on another MDT). In the event of a conflict, the system shall notify the vehicle operator of an “invalid” logon. If the operator ID and run ID received from the MDT are valid, a message shall be sent to the MDT indicating whether the logon attempt was successful or failed.

Once the operator and run IDs have been validated, the MDT shall complete the logon by selecting the schedule/manifest data stored in the MDT that corresponds with that run/trip. The system shall provide dispatchers the ability to manually logon a vehicle operator to an appropriate run.

After logon, the operator terminal shall display the current run, route, trip, next time point, and vehicle operator ID.

The MDT shall track whether or not a wheelchair lift was cycled (if applicable) before the vehicle is moved an agency configurable distance after logon, and report to central software in real time if it was not cycled.

The MDT shall allow the vehicle operator to logoff by selecting the logoff key. The MDT shall send a message to the dispatcher as a confirmation of the vehicle operator logoff. The MDT shall periodically attempt to send a logon or logoff message until it receives an acknowledgement message from the central system, or if no response is received from the central system within a TP-configurable time, the MDT shall provide the operator with a “no logon response” message, and the system will continue to attempt to send the logon or logoff message.

116 Electronic Pre- and Post-Trip Inspection

Upon successful login, the MDT shall present the vehicle operator with a pre-trip checklist. The pre-trip checklist shall be configurable by each TP and shall be designed to prompt the vehicle operator to confirm that pre-trip procedures were performed. The pre-trip screen shall include
standard pre-trip procedures as defined by each TP. A log of the pre-trip input shall be transmitted to and retained in the central system database. The MDT shall provide an electronic interface to record results of the pre- and post-trip inspections to be conducted by drivers. The Contractor shall design the inspection forms in coordination with the RTRC to comply with existing inspection process. The inspection forms shall provide the capability for drivers to record their “electronic signatures,” allowing the vehicle operator to submit an electronic signature or other text to the central system using a finger or stylus. The system shall record the driver id, vehicle id, location (where the vehicle is parked or garaged) id and date and time of form completion once form is electronically signed. The inspection data shall be automatically uploaded to the central system in real-time and shall be available to the authorized staff to review as needed.

117 Geo-fencing

The system shall provide the ability to define geo-triggers around pre-defined locations in the RTRC service area. The system shall allow each TP to associate geo-triggers with specific actions. The actions shall be activated when vehicle enters the defined geo-trigger and shall deactivate as soon as the vehicle leaves the geo-trigger.

118 Vehicle Location Tracking

119 GPS Receiver and Antenna

The GPS receiver shall report date and time, latitude, longitude, speed, direction of travel and whether or not the receiver has a GPS position lock. The GPS receiver shall be at least eight channel parallel tracking receivers, capable of simultaneously tracking at least four GPS satellites in the best available geometry, while also tracking at least the four next best and/or upcoming (rising) satellites. The on-board GPS receiver must be Wide Area Augmentation System (WAAS)-capable, providing position accuracy within ten feet (or three meters) 95 percent of the time. In the event that the GPS receiver is not WAAS compliant, the Proposer shall indicate how the GPS accuracy requirement is met. The GPS receiver shall have a cold start solution time of 60 seconds or less and a re-acquisition time of 15 seconds or less. Velocity measurements provided by the GPS equipment shall be accurate to within 0.3281 feet (0.1 meters) per second. The MDT shall utilize an internal GPS antenna or shall be integrated with a GPS antenna securely mounted on the exterior of the vehicle. If mounted externally, the antenna, mounting and sealants shall be impervious to physical and chemical penetration by automatic vehicle washing equipment. The Contractor shall interface with vehicle odometers and provide a gyroscope to compensate for the loss of GPS signals. In the event that location data is not available from GPS receiver, the MDT shall be able to calculate vehicle location based on vehicle speed, odometer readings and gyroscope data.
120  
**Location Reports**

MDTs shall send a location report to the central system immediately when polled by the central system, or automatically once a configurable number of minutes have passed since the previous location report. All transmitted data shall be stamped with following information: date and time, “GPS lock” status, latitude and longitude, heading, run number, vehicle number, and vehicle operator ID number.

121  
**Location Tracking**

The system shall receive location reports from vehicles at a configurable time period as determined by the TPs. The system shall receive and store latitude and longitude information stamped with date, time, vehicle, vehicle operator, run, and trip information from MDT’s. The display shall provide an indication if the last reported location being displayed is older than the reporting interval. In the event when location of a vehicle on the AVL map is shown to be older than a minute, the system shall allow the dispatcher to manually poll/locate a vehicle. The system shall display on the map the last reported location for all vehicles, using an icon indicating vehicle direction and labeled with the vehicle ID, trip ID or operator ID as selected by the user. The time interval at which location reports are received shall be configurable by each TP.

122  
**Location Playback**

TP staff shall be able to review on the map display the chronological sequence of reported locations for a specified vehicle(s) over a specified time period. The software shall provide controls to view the entire sequence of reported locations from the beginning of the time period or to step through the sequence incrementally forwards or backwards.

The replay data shall include location reports and schedule adherence status. The system shall allow replay for a single vehicle, selected set of vehicles or all vehicles on the selected map view for selected time period. The system shall allow selection of any time period for the historical data stored in the database. The system shall be able to store a playback in a format that can be exported for viewing on any computer.

123  
**Canned Data Messaging**

The MDT shall not allow vehicle operators to send or view a canned data message when the safe driving mode is enabled on their vehicles. The MDT shall allow the vehicle operator to send a canned data message to the central system by selecting from a set of pre-defined messages. All canned messages to dispatch shall include the date, time, location (latitude and longitude) and odometer value. When a canned data message is received from dispatch and available for viewing, the MDT shall indicate this with a distinct audible tone and visual alert.
The system shall allow for any message sent by dispatch to be flagged as requiring vehicle operator acknowledgement, a Y/N response and shall allow the dispatcher to view a list of such messages that have not yet been acknowledged.
The MDT shall store up to a configurable number of canned data messages received from dispatch, indicate to the vehicle operator when there are unread text messages, and allow stored messages to be viewed or deleted. The MDT shall allow the vehicle operator to view received messages that are longer than can fit on one line of the display.
The MDT shall allow the vehicle operator to send an acknowledgement or Yes/No response to certain messages received from the central system.
The MDT shall periodically attempt to send a canned data message or response until it receives an acknowledgement message from the central system.
The system shall allow the dispatcher to view received canned data messages in a tabular display that also indicates the vehicle ID and the time of the message.
The system shall allow the dispatcher to send a message to a single MDT, a predefined group of MDTs, all MDTs within an area selected on the map display or all MDTs operating.
The system shall be configurable to allow for audible and visual alerts for incoming messages.
The system shall allow the dispatcher to select one of a set of predefined messages (canned data messages) or enter a free text message.

124 Manifest Management

Manifests and manifest updates sent by a dispatcher shall be displayed on the MDT screen. The screen shall display upcoming pickup or dropoff trip events in summary format including at least event type (e.g., pickup, dropoff), arranged pickup time, appointment time (if applicable), client name, gender, event location, fare or co-pay amount (if appropriate), mobility assistance requirements, image of the client, and other pertinent information, as determined by each TP.
The MDT shall allow the vehicle operator to select a trip event to get full detail on the pickup or dropoff on a separate screen, which shall include, at a minimum, pickup/dropoff, first and last name, client id, gender, appointment time, pickup time, location, location comments, fare or co-pay amount, fare type, number of passengers and Personal Care Attendant (PCA).
The MDT shall request manifest data from the TCSDS on a periodic, ongoing basis to display at least the next 10 trip events or trip events scheduled in the next 60 minutes, with these thresholds being configurable by each TP.
The MDT shall not allow a request for no-show until a TP-configurable time interval has passed after the ‘arrive’ trip event or the start of the customer pickup time window, as determined by each TP.
Once any of these trip events are selected on the MDT, the MDT shall send a message including the date, time, and location to the central software.
The MDT shall require that the vehicle operator acknowledge the receipt of an insertion, deletion or change to the current manifest (including no-show events). There shall be an audible tone from the MDT when any such manifest change notification is received. All changes in the manifest will be highlighted in distinct colors.

125 Trip Events
The MDT shall send a corresponding message to the TCSDS when the vehicle operator selects a pull-out, pull-in, pickup, no-show requests, no-show event (after requesting a no-show from dispatch), or dropoff trip event.

The operator shall use the MDT to select an ‘arrive’ event by pressing a button when first arriving at the location, and then again use the MDT to select a ‘perform’ event when about to depart the location. The vehicle must not be in motion to select ‘arrive’ and ‘perform’ events. In the case of grouped trip events, the vehicle operator shall register a single ‘arrive’ event. The MDT will be configured to not allow the ‘arrive’ event unless the vehicle reaches within configured radius of the pickup location.

If the customer is not available at the location, the operator shall use an MDT button to request a ‘no-show’.

Pickups with a pending no-show request or that have been cancelled due to a no-show shall be indicated to the dispatcher.

The MDT shall not allow a request for no-show until an agency configurable time interval has passed after the ‘arrive’ trip event or the start of the customer pickup time window, whichever is later.

Once any of these trip events are selected on the MDT, the MDT shall send a message including the date, time, location and odometer value to the central software.

The operator shall have the opportunity to update the fare type at the time of selecting the perform trip event and send the updated information to the TCSDS.

The trip event message shall include the date/time, trip event type, location and odometer value. Prior to sending the trip information, the operator shall be allowed to verify and adjust the odometer value for that trip.

The MDT shall continue to periodically attempt to send a trip event report until it receives an acknowledgement from the central software that the report was received.

126  **MDT-Odometer Interface**

The MDTs shall be interfaced with the existing odometer, receiving the digital or analog signal and determining the distance traveled since the MDT was logged on, including the ability for the TP to adjust the odometer calibration. In the event when the GPS-odometer is proposed to be used in place of vehicle odometer, Proposers shall provide the documented evidence of GPS-odometer accuracy in their proposals.

The accumulated mileage data collected by MDTs shall be calibrated to be within 5% of observed mileage.

127  **Real-time Customer Information**

Proposers shall describe their proposed system’s ability to independently provide or export through a standard protocol, appointment reminders to TP staff and clients. The time period (e.g., X hours before a scheduled appointment) and format (e.g., Text Message, Automated Phone Call, etc.) in which reminders are provided shall be configurable by each TP or client.

128  **Predicted Arrival Time**

The system shall have the ability to dynamically generate and update the predicted arrival times for in-service TP vehicles.

The system shall be able to account for at least the following operational anomalies in making corrections in the predicted arrival times:

- Travel time variability by day and time of day;
• Service disruption (e.g., vehicle breakdown or weather-related disruption) and detours; and
• Driver logon/logoff error.

129  Web-based Trip Status
The system shall allow customers/relatives to view the status of their trip on the RTRC or TP website or web-enabled personal devices. Registered customers shall be able to view the status of their trips by logging onto their profile.
The system shall allow customers to view the location of their vehicles on a map-based interface.

130  Email/Text Alerts
The system shall be able to send emails to customers based on their trip preferences.
The system shall be able to send text message to customers based on their trip preferences.
The system shall have the ability to respond to customer requests for real-time status of a prescheduled trip.

131  Interactive Voice Response (IVR) Alerts and Reservation Access
The TCSDS system shall have the ability to interface with an IVR system to provide customer alerts regarding ride reminders and real-time arrival information via IVR system.
The IVR shall allow customers to cancel their trips using a series of prompts to identify their trip reservation, cancel the reservations and confirm the cancellation.

132  General
The IVR system shall provide the capability for customers to access and be contacted with information about RTRC and TP services and reservations via telephone. The Contractor shall be responsible for supplying hardware and software, technical support, and warranty coverage on implemented hardware and software.
The IVR system shall be interfaced with the TCSDS and predicted arrival time (described above) to provide current predicted arrival time for customers 30 minutes prior to the predicted arrival time.
The IVR shall contact customers with a reminder call about their trip the day before service. If a customer’s trip is predicted to be delayed by more than a configurable number of minutes, the IVR shall contact the customer with an updated arrival time.
The Proposer shall indicate how the IVR system will be compliant with FCC Section 255 of the Communications Act and Limited English Proficiency requirements.
The system shall provide both a web- and phone-based customer interface for registering with the IVR system.

133  Phone System Integration
The IVR shall be integrated with the existing telephone system at the RTRC. Proposers shall describe and provide cost of any needed upgrades in the existing phone system to meet the IVR functionality.

134  Customer Interface
The customer interface shall consist of voice prompts to which the customer may respond by either voice commands or by touch-tone key selection.
The IVR system shall provide a welcoming message as its first response to incoming callers or call recipients. The system shall allow for an additional optional message to be spoken after the welcome message.

The IVR system shall be designed such that incoming calls with no touch-tone or voice response within a short period of time by the customer are acted upon automatically (time-out). Proposers shall specify proposed options for calls that time-out or for which there is no touch-tone service. The voice prompts shall encourage incoming callers to use the automated menu-based interface as a first choice over communication with a live Customer Service Representative. The voice system structure shall provide key-ahead of touch-tone inputs such that experienced users do not have to wait for voice messages or prompts to complete prior to making a touch-tone or voice selection.

At any time during the call, the customer may request a transfer to the RTRC Customer Service via touch-tone key or voice command. The touch-tone key used for this particular selection shall remain consistent throughout the customer interface.

135 Call Transfers

The proposed system shall handle at least 2,500 calls per day. Please note that this call volume may have to be increased once there is an understanding of the actual average daily number of calls.

The proposed IVR system shall be capable of transferring calls to RTRC Customer Service. When a transfer request to Customer Service is initiated by a caller after business hours, the IVR system shall provide an informational message to the caller and then return the caller to the first level of the IVR system voice menu. When a transfer request to Customer Service is initiated by the caller during regular business hours, the IVR system shall transfer the caller to Customer Service if a call taker or queue space is available. When a transfer request to Customer Service is initiated by the caller during regular business hours but when call takers are busy and the queue is full, the IVR system shall detect the queue-busy condition, hold the call, announce the approximate amount of time the caller may be on hold and provide IVR menu options for automated assistance.

136 Usage Data Collection and Reporting

The IVR system shall collect customer call data and provide reports for administrative purposes. The Contractor shall describe the level to which data may be collected for incoming customer calls and for the touch-tone responses to menu options. The proposed system shall allow a system administrator to generate reports for specific time periods, including the following types of reports:

- Number of total incoming calls;
- Number of calls that transfer to Customer Service; and
- Call duration for each call.

The proposed IVR shall allow the system administrator the capability to generate the above reports by the following selectable periods: hourly, daily, range of days, weekly, monthly and yearly.
The proposed IVR system shall provide the capability for the system administrator to record and edit vocabulary words, and construct the phrases that will be used by the IVR system. The Contractor shall specify the method(s) for recording and editing vocabulary words, and constructing phrases.

The proposed IVR system shall provide speech editing features. The Contractor shall specify features supported by the vocabulary management environment, including but not limited to:

- Individual vocabulary edits;
- Pause deletions and insertion; and
- Undo/redo individual vocabulary edits.

The IVR system shall provide the capability to store and manage all vocabulary words and phrases used by the system. Contractor shall describe how the vocabulary words and phrases are to be stored and managed.

138 Future Capabilities
The RTRC has identified future or optional functionality of the TCSDS, including the following:

- Providing an account-based electronic fare payment system;
- Billing funding sources using electronic billing requiring electronic data interchange (EDI); and
- Exchanging information with other scheduling and dispatching systems using the Transactional Data Specification (see Section 6.6 and http://www.trb.org/Main/Blurbs/180593.aspx).

Proposers are required to identify their capabilities as they relate to providing each of these future or optional functionalities.

139 Project Implementation
140 General
The Contractor shall prepare all deliverables in both Microsoft Office (Word, Excel or PowerPoint) and Adobe PDF formats, with the RTRC and TPs granted full rights to reprint as needed.

141 Required Project Schedule
Table 4 shows the required schedule of activities and deliverables that will be described in subsequent subsections.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Time Since Last Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Preliminary Design Document (PDD)</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>6</td>
<td>Preliminary Design Review (PDR) Meeting</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>7</td>
<td>Final Design Document (FDD)</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>8</td>
<td>Final Design Review (FDR) Meeting</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>9</td>
<td>FDD Approval</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>10</td>
<td>Acceptance Test Procedures (ATP) for Factory Acceptance Test (FAT)</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>11</td>
<td>FAT</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>12</td>
<td>FAT Punch List, FAT Results Document and FAT Approval</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>13</td>
<td>Resolve FAT Punch List</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>14</td>
<td>Training Manuals and Training</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>15</td>
<td>ATP for Pilot/Installation Testing</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>16</td>
<td>Pilot/Installation Testing</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>18</td>
<td>Resolve Pilot/Installation Testing Punch List</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>19</td>
<td>ATP for System/User Acceptance Testing</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>20</td>
<td>System/User Acceptance Testing</td>
<td>3 Weeks</td>
</tr>
<tr>
<td>22</td>
<td>Resolve System/User Acceptance Testing Punch List</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>23</td>
<td>Burn-in/Rigorous Testing</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>24</td>
<td>Burn-in/Rigorous Testing Results Document and Burn-in/Rigorous Testing Approval</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>25</td>
<td>Resolve Burn-in/Rigorous Testing Punch List</td>
<td>2 Weeks</td>
</tr>
<tr>
<td>26</td>
<td>Final System Acceptance</td>
<td>2 Weeks</td>
</tr>
</tbody>
</table>

142 Project Management

143 Project Status Tracking

The Contractor shall prepare a System Implementation Plan (SIP), including detailed implementation activities and a schedule for these activities, the roles and responsibility of parties (Contractor, RTRC, TPs and other parties) in the proposed project team, progress milestones and status, and assigned Contractor staff.

Proposers must submit their data conversion plan as part of the draft SIP provided in the proposal. Potential risk items and their resolution must be clearly identified per the Proposers’ prior experience with similar implementations.

The initial draft of the SIP shall be provided to the RTRC within two weeks from Notice to Proceed (NTP).
The Contractor shall participate in a kickoff meeting with the RTRC Project Manager, other RTRC and TP staff, and outside consultants as determined by the RTRC Project Manager. The SIP shall be discussed at the kickoff meeting. After the kickoff meeting, the SIP must be revised by the Contractor based on comments made during the kickoff meeting and by the RTRC and TPs. The revised document shall be provided to the RTRC within two weeks after the kickoff meeting. Please refer to Table 4 for recommendations on high-level tasks that should be included in the SIP.

Also, the Contractor shall include a Safety Management Plan in their SIP, which shall detail their responsibilities and procedures for safety during the different phases of the project, including (1) conducting pre-installation surveys to identify potential project safety hazards; (2) identifying project hazard control procedures, including occupational (worker) and public hazards; (3) providing project safety orientation and training to its subcontractors and RTRC/TP staff who will be involved in the project; and (4) furnishing procedures and training for project accident reporting and investigations.

The SIP must be approved and accepted in writing by the RTRC before it can become effective. An updated SIP shall be submitted to the RTRC at the beginning of each month, until project completion and system acceptance by the RTRC.

The SIP shall include a rollout plan for all RTRC-dedicated vehicles.

The Contractor shall maintain and provide to the RTRC an Action Items List (AIL), indicating for each item the following: (1) item number; (2) date generated; (3) item priority; (4) brief item descriptive title; (5) assigned person with lead resolution responsibility; (6) date resolved; and (7) ongoing dated notes on resolution status.

The AIL shall be sorted, primarily by unresolved vs. resolved items, priority, and by the date the item was generated. The RTRC reserves the right to negotiate additional items for the AIL prior to formal acceptance.

**144 Bi-Weekly Conference Calls**

The Contractor shall participate in bi-weekly conference calls with the RTRC Project Manager, other TP staff, and outside consultants as determined by the RTRC Project Manager.

The agenda for these meetings will be to discuss the most current status of and plans related to all issues identified in the recent releases of the SIP and AIL.

The RTRC reserves the right to identify for discussion any additional issues beyond those in the SIP and AIL.

A status report shall be issued to the RTRC at least two days prior to each conference call, including (1) an agenda for the upcoming conference call highlighting key discussion items; and (2) an updated AIL with the updates incorporating the discussions of the previous bi-weekly conference call as well as other subsequent developments since the previous AIL release.

The Contractor shall be represented in these conference calls by at minimum their Project Manager, as well as any additional Contractor staff necessary to properly address the current issues and project status.

The RTRC will be represented by their designated implementation management representatives. Outside consultants may attend or participate in all conference calls, as needed.

Conference call facilities will be arranged and paid for by the Contractor.

The Contractor shall submit minutes of the call within two days of each conference call. The minutes shall be included as a task on each AIL submitted following a conference call.
Minimum Required Onsite Work
At the first onsite meeting, which is the Kickoff Meeting/Requirements Review (see Table 3, Item 3), the Contractor shall be prepared to discuss the RTRC’s feedback on the draft SIP and conduct a Requirements Review (RR).
At the second onsite meeting, which is the Preliminary Design Review (PDR), the Contractor shall be prepared to discuss the RTRC’s feedback on draft Design Review documentation. During the third onsite meeting, which is the Final Design Review, the Contractor shall present the Final Design Review documentation for review. Based on discussion at this meeting, the Contractor shall make any final revisions to the FDD.
During subsequent onsite efforts, the Contractor shall install the system, configure system access and conduct acceptance testing. These onsite installation, system configuration and testing efforts will occur over an extended period, and will likely involve several different onsite trips and a range of different Contractor staff.

Invoicing
The Contractor shall only submit an invoice once a fully-signed Acceptance Certificate is generated by the RTRC indicating that a progress payment milestone has been achieved. The RTRC will withhold 10% retainage on each invoice. Upon system acceptance by the RTRC, the total retainage will be paid to the Contractor.

Design Reviews
Requirements Review (RR)
The Contractor shall participate in the RR, as part of the first onsite meeting. The RR will initialize the Requirements Matrix (RM) and the Contractor will use this Matrix to produce the draft Design Document for conducting the Preliminary Design Review (PDR) at the second onsite meeting. The RR meeting shall discuss, for each contract requirement, the following: (1) the RTRC design intent; (2) the intended Contractor design approach; and (3) the general Contractor approach to demonstration through the acceptance testing process.
Finalized contractual requirements will be prepared after the RR meeting and will be referred to as the Requirements Matrix hereafter.

Preliminary Design Review
There shall be two design reviews in which the Contractor must participate. For the design reviews, the Contractor will be required to prepare comprehensive documentation on the technical details of the system before proceeding with the installation. The design review materials to be prepared by the Contractor will include overall system documentation, details for installation with each vehicle type/site and fixed facility, and an itemization of how their design responds to each individual specification requirement. An important principle with the design review process is that the RTRC acceptance of the design review documentation will not represent acceptance of the system, which can only result from successful system acceptance testing.
The beginning of the design review process is a Preliminary Design Review (PDR) meeting, which deals with the Contractor’s initial version of the system design. This meeting is an important opportunity to identify any misunderstandings of the design intent and to adapt the design within the Contractor’s constraints to best suit the RTRC’s needs.
The Contractor shall prepare the Preliminary Design Document (PDD), which shall include the following materials: (1) a conceptual diagram illustrating all elements in the system and data flow will be required; (2) an overview of the equipment, system and configuration proposed for implementation; (3) detailed technical documentation for each equipment item; (4) detailed
technical documentation on all software, addressing the functions of each module, the format of all user interface screens, the format of all reports, the data fields to be included in all data exchange interfaces and any other software aspects warranting advance agreement with the RTRC prior to system customization/configuration; and (5) a table providing cross-references for each section of the PDD to the appropriate element of the RM.

The RTRC shall review the PDD in advance of the PDR meeting, and finalize their review and comments on the PDD after the PDR meeting is held.

150 Final Design Review

The second step in the design review process is a Final or Critical Design Review (FDR), which deals with the Contractor’s final system design, based on the results of the PDR and updated RM. The FDR meeting involves consensus building in an onsite meeting or conference call once the design is finalized.

Based on comments made by the RTRC on the PDD, the Contractor shall make revisions to prepare the final design document (FDD).

The FDD shall include the following materials: (1) updated PDD incorporating RTRC feedback and comments; (2) final list of equipment to be procured; (3) final design and configurations of the system to be built including all customizations to be made to the system; (4) an updated table providing cross-references between sections is the FDD and elements of the RM; and (5) updates to the Project Schedule.

The Contractor shall conduct the FDR onsite or via conference call three weeks after the FDD has been submitted.

The PDD and FDD are intended only to reduce the chance of any misunderstandings on the design intent or interpretation of the contract requirements. The PDR and FDR shall not alter the need for the successful formal demonstration of each requirement through the Acceptance Testing process.

Once the FDD is complete and accepted by the RTRC, the Contractor shall provide a detailed list of equipment for the system.

The Contractor shall create a detailed list of system configurations. An example of these configurations is a list of canned messages, and list of incidents and accidents codes.

The Contractor shall document configurations of the computer hardware and networking infrastructure as part of the FDD.

151 Testing

The Contractor shall submit an Acceptance Test Procedures document (ATP), for the RTRC approval prior to undertaking any testing.

The ATP shall clearly address: (1) how each testable contract requirement (listed in the RM) will be demonstrated, including the method for performing the test; (2) the results that will constitute success for each test; (3) responsibilities of both Contractor and the RTRC’s representatives during each test; and (4) a cross-reference to which contract requirements from the RM are being addressed by each test procedure.

The ATP shall include an updated RM from the design review documents, to include the test stage at which each contract requirement will be demonstrated; and a cross-reference to the test procedure(s) that serve to address each contract requirement.

The ATP document shall be submitted to the RTRC at least three weeks in advance of any intended testing.
The ATP shall reflect the following distinct testing stages for the proposed system: (1) Factory Acceptance Test (FAT); (2) Pilot Testing/Installation Testing; (3) System/User Acceptance Testing; and (4) Burn-in/Rigorous Testing.

FAT shall be completed before the equipment and software is shipped to the RTRC and TPs for installation, and deficiencies shall be rectified before shipping to the RTRC and TPs for installation.

FAT shall be witnessed by the RTRC’s and TP representatives (RTRC and TP staff and/or designated support consultants).

Pilot/Installation Testing shall be completed for at least one type of each vehicle in the RTRC-dedicated fleet, for any on-board systems. Installation testing will include the Contractor, working with the RTRC’s IT staff, installing the RTRC’s databases and the Contractor’s software, and operating the system in a test environment. Pilot and installation testing will be conducted on-site at the RTRC. The Contractor will be required to submit proposed test procedures, which will need to include a cross-referencing to identify which procedure(s) demonstrate each requirement from the Requirements Matrix (RM). Any deficiencies observed in a four-week period following Pilot/Installation testing shall be rectified before the initiation of System Testing (ST). Vehicles used during Pilot Testing will be in operation for four weeks to observe issues that arise in daily operations.

Prior to commencement of Pilot/Installation Testing, the Contractor shall validate scheduling parameters and on-board data configurations to ensure that they are reasonable and accurate. Pilot/Installation Testing shall be witnessed by the RTRC and TP representatives.

System/User Acceptance Testing shall be completed after the entire system has been installed, and deficiencies shall be rectified before the initiation of Burn-in/Rigorous Testing.

System/User Acceptance Testing will include operating the system using live data. This testing stage will be conducted on-site at the TPs. The Contractor will be required to submit proposed test procedures, which will need to include a cross-referencing to identify which procedure(s) demonstrate each requirement from the Requirements Matrix (RM).

System/User Acceptance Testing shall include the testing of all spare components.

System/User Acceptance Testing shall be witnessed by the RTRC and TP representatives.

Burn-in/Rigorous Testing shall involve revenue service use of the system over a 30-day period after the completion of System/User Acceptance Testing, and deficiencies shall be rectified before the RTRC will grant Final System Acceptance (SA) for the system. This testing stage will be conducted on-site. The Contractor will be required to submit proposed test procedures, which will need to include a cross-referencing to identify which procedure(s) demonstrate each requirement from the Requirements Matrix (RM).

The RTRC may authorize the Contractor to proceed to the next testing stage with certain deficiencies not yet resolved.

The Contractor shall provide written notice to the RTRC at least two weeks in advance of any testing, indicating the specific tests to be completed. The Contractor will coordinate the date, time and location of testing to minimize disruption of service.

The Contractor shall be required to reschedule testing if the RTRC witnessing representatives cannot be present or if other circumstances prevent testing from taking place.

The Contractor shall provide written Test Results Documentation (TRD) after completing each stage of testing.

The TRD shall document the results of each ATP procedure and provide an updated RM that indicates which contract requirements have been demonstrated.
The TRD must be approved before the RTRC grants System Acceptance. System Acceptance will not be granted for the system until all contract requirements have formally demonstrated through Burn-in/Rigorous Testing. The RM shall be used as a “punch list” to track which requirements have not yet been demonstrated at each stage of testing.

A requirement classified as having been “demonstrated” during a certain testing stage can be subsequently redefined as having been “not demonstrated” if compliance issues emerge prior to System Acceptance.

152  Documentation
The Contractor shall provide an As-Built Document (ABD) to the RTRC for approval. The ABD shall include: (1) an inventory of all on-board components supplied including supplier, model number, serial number and installation location; (2) an inventory of all spare on-board parts supplied including supplier, model number, serial number and storage location; (3) all reference and user manuals for on-board system components, including those components supplied by third parties; (4) all warranties documentation, including that for on-board components supplied by third parties; (5) a diagram indicating the as-built interconnections between on-board components; and (6) the version number of all software, including that supplied by third parties.

The Contractor shall provide Maintenance Manuals documenting (1) how the on-board system components were installed; (2) how to install and configure spare on-board components; and (3) the schedule/procedures for preventative maintenance, inspection, fault diagnosis, component replacement and warranty administration on each on-board system component.

The Contractor shall provide User Manuals (UMs) for the users of the TCSDS system, documenting use of all functions of the software.

The Contractor shall provide Vehicle Operator Manuals documenting use of the MDTs and on-board equipment.

The software application shall include context sensitive help capability.

The Contractor shall provide a Systems Manuals (SMs), documenting (1) the configuration of the TCSDS system hardware and software; (2) TCSDS system functions and operations; (3) scheduled maintenance required for the TCSDS; and (4) database structure and data dictionary. The Contractor must provide disaster recovery documentation highlighting how system can function and prevent any data loss in the event of a natural disaster or other unexpected events.

153  Training
The Contractor shall provide training courses for at least the following positions:

- Reservationist / Scheduler / Dispatcher
- Administrative Staff
- System administrator/IT staff
- Vehicle operators
- Customer service representative;
- Systems administrator;
- Database Managers
- Managers
The RTRC will provide the actual number of staff for each of the above categories of trainees.
The Contractor will describe the necessary pre-requisite computer skills and knowledge expected for each of the training courses in order to develop training classes based on user skill level.
The Contractor shall provide all training materials in either Microsoft Office or Adobe PDF formats with a permission to reproduce copies later on.
The Contractor shall provide additional training to the original trainees after Final System Acceptance for the system at no additional cost if major modifications are made to the system after the initial training due to system upgrades or changes made under warranty; and/or Final System Acceptance occurs at least three months after the completion of training, due to delays for which the Contractor is responsible.
The Training Plan, including the training schedule and course outlines, must be provided to the RTRC for review at least three weeks in advance of the start of training. Training must be conducted prior to the User Acceptance Testing.
Each Proposer shall provide a sample Training Plan with the following details in their proposal:
- Total number of onsite training sessions proposed;
- Total number of web-based training session proposed;
- List of training courses;
- Number of classes per course;
- Maximum number of attendees per class; and
- Number of follow-up sessions (specify on-site or web-based) or itemize cost per session.
The Training Plan must be approved in writing by the RTRC before the start of any training.
The Contractor shall furnish all special tools, equipment, training aids and any other materials required to train course participants, for use during training courses only.
The instructors shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead students in a classroom setting.
If any instructor is considered unsuitable by the RTRC, either before or during the training, the Contractor shall provide a suitable replacement within five business days of receiving such notice from the RTRC.
The Contractor shall provide brief refresher versions of each training course to the original trainees between three to six months after System Acceptance of the system at no additional cost.
During the warranty period, the Contractor shall provide additional training to the original trainees after System Acceptance for the system at no additional cost if major modifications are made to the system after the initial training due to system upgrades or changes.
The Proposer shall provide the cost of additional training for staff after the System Acceptance period (new hires, etc.) on the Price Proposal Form.

154 Warranty and Spares

155 Warranty

The Contractor shall provide a single point of contact for all warranty administration during the warranty period.
The Contractor shall confirm that it has reviewed and evaluated all information furnished by the RTRC and has made all inquiries necessary such that the Contractor is fully aware of the RTRC’s business requirements and intended uses of system, as set forth or referenced in the Request for Proposals (RFP) and any Addenda, Amendments or Final Proposal Requests, as well as in discussions held previous to the Proposer’s submission of the proposal and during the Pre-proposal Conference.
The Contractor shall warrant that the system satisfies the foregoing requirements in all material respects and will be fit for such intended uses.
The Contractor shall warrant that the design, materials, construction, software and workmanship of the equipment shall reflect the intended use of the equipment as a component of the overall human service transportation management system in the HSTC Region 9 environment.
The Contractor shall warrant that equipment and software, including the initial supply of spare
components, (1) are free from defects in design, material and workmanship, and shall remain in good
working order, and (2) function properly and in conformity with this Contract.
The Contractor shall provide any software updates and patches for the current software version at no cost
to the RTRC or TPs during the warranty period.
The Contractor shall warrant that the RTRC and TPs shall acquire permanent title to all equipment and
non-proprietary software provided under the Contract, free and clear of all liens and encumbrances.
The warranty period for the system shall run concurrently for all system components from the date of SA,
through to five (5) years from the date of SA, although the warranty must assure that data is available for
a minimum of seven years.
Proposers shall offer pricing for an option to extend the warranty period for the system for additional
years beyond five years. The RTRC and TPs may include an extended warranty in the contract with the
Contractor. Proposers shall itemize the cost of each extended warranty period and document any
differences in the warranty terms for these option years in their proposal.
Proposers shall describe the pricing and services offered as part of different levels of support available
(e.g., basic, advanced and premium levels of support).
The Contractor shall warrant that the documentation provided shall completely and accurately reflect the
operation and maintenance of the equipment and software, and provide the RTRC and TPs with all
information necessary to maintain the system.
If there is a change in the production configuration of any equipment or software being installed prior to
Final System Acceptance, the RTRC and TPs may require that all previously installed equipment and
software be upgraded to match the updated configuration.
The Contractor shall warrant compliance with all applicable laws and regulations relating to the project.
During the warranty period, the Contractor shall, at no cost to the RTRC or TPs, furnish such materials,
labor, equipment, software, documentation, services and incidentals as are necessary to maintain the
system in accordance with the warranty.
The Contractor shall warrant that its employees, agents and Subcontractors assigned to perform services
under this contract shall have the proper skill, training and background to perform in a competent and
professional manner, and that all work will be so performed. The RTRC and TPs reserve the right to
remove any subcontractors if their work is deemed incompetent or unprofessional.
In addition to the foregoing warranties, the Contractor shall assign to the RTRC, and the RTRC shall have
the benefit of, any and all subcontractors', suppliers', and vendors' warranties and representations with
respect to the deliverables provided.
In its agreements with subcontractors, suppliers and vendors, the Contractor shall require that such parties
(1) consent to the assignment of such warranties and representations to the RTRC; (2) agree that such
warranties and representations shall be enforceable by the RTRC in its own name; and (3) furnish
documentation on the applicable warranties to the RTRC.

156 Repair or Replacement of Faulty Components
During the warranty period, the Contractor shall repair or replace any faulty components, with the cost
included in the warranty price. The RTRC and TPs will ship each faulty component to the Contractor,
who shall return a new or repaired component within one week of originally receiving it.
If the Contractor determines that a returned component is not faulty, the RTRC and TPs shall receive the
original component back in working order within two days of the Contractor originally receiving the
returned component.
All components received back at the RTRC and TPs from the Contractor will be tested in accordance with
the original ATP, and returned to the Contractor if faulty accompanied by a certification.
The Contractor shall pay all shipping charges to and from the RTRC and TPs, and any duties associated
with the repair or replacement of faulty units.
Returned or replaced spare components shall be packaged, organized and labeled in the same manner as
the original supply of spare components.
157  System-wide Replacement
If at least 25% of a given component requires repair or replacement within the five-year warranty period, the component shall be deemed to warrant system-wide replacement.
System-wide replacement shall require the Contractor to replace all units of the suspect component throughout the system, whether or not they have exhibited any fault.
Even if the system-wide replacement activity extends beyond the end of the five-year warranty period, the Contractor shall be obligated to complete it if the need was documented before the end of the warranty period.

158  Spare Components
The Contractor shall provide an initial supply of spare components to the RTRC and TPs for all installed hardware (e.g., tablets if procured from the Contractor), with a quantity of at least 10% of the installed quantity (with a minimum quantity of 1).
Spare parts for TPs’ hardware must be housed in a location that is easily accessible to each TP.
The location of spare parts for the RTRC has not yet been determined. The proposal shall include a list of the spare components and quantities to be provided, including manufacturer, model numbers and unit prices. At any time during the warranty period, the RTRC and TPs shall be able to purchase additional spare components at the unit price stated in the price proposal form.
Spare components shall be delivered to the RTRC and TPs already organized and labeled such that they can be readily identified and found. The organization and labeling must be approved by the RTRC’s Project Manager.
Spare components shall be fully configured, including any license requirements, so that they may be immediately utilized in the event of component failure.
Spare components shall be packaged to protect their reliability, including providing for them to be identified, inspected, stored for long periods, and endure multiple inventories without damage or degradation.
Additional spare components purchased during the warranty period shall be packaged, organized and labeled in the same manner as the original supply of spare components, although additional storage provisions will not need to be provided.

ODOT is in the process of developing a Service Level Agreement (SLA) for getting spare parts in a timely manner. The Proposer shall provide a sample SLA that addresses this need.
Invitation No. 524-23

State of Ohio, Department of Transportation (ODOT)
Office of Contract Sales, Purchasing Services

Terms and Conditions for Submitting Excel Pricing File in Bid Package
(Last Revised 07/2020)

1. DOWNLOADING THE EXCEL PRICING FILE: Bidders can access and download the most current Excel Pricing File for this procurement by following the hyperlink provided below:

http://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/PurchDocs/524pricing.xlsx

2. SUBMISSION OF EXCEL PRICING FILE: Bidders should submit the pricing page in the original excel format.

3. UNAPPROVED ALTERATIONS TO EXCEL PRICING FILE: Bidders who materially alter the original content of the Excel pricing file (e.g. specifications, formulas, etc.) issued by the Department may be found non-responsive and ineligible for award of this procurement.

4. CHANGES TO EXCEL PRICING FILE: The Department will only make modifications to the Excel pricing file by written addendum only. Where changes are necessary to the Excel pricing page, the Department will issue a new Excel pricing page indicating the revisions made and a revision date for the changes.

   It is the sole responsibility of the bidder to check for issued addenda prior to submitting a bid package to ensure the most updated Excel pricing file is being utilized.

5. DESCRIPTIVE LITERATURE: Bidders may electronically provide any descriptive literature (e.g. brochures, spec/cut sheets, drawings, MSDS, etc.) regarding the products and/or services offered by the bidder. As this literature may be publicly posted for viewing by purchasers, bidders must not submit any literature electronically in which they consider to be a trade secret, proprietary, or confidential in any way.

   (the remainder of this page has been left intentionally blank)
1. **BIDDER REGISTRATION**: The Department requires awarded bidder(s) to successfully register as a State of Ohio Supplier with the Department of Ohio Shared Services and successfully obtain an OAKS vendor identification number (OAKS ID) within fourteen (14) calendar days from the date of contract award and execution. The Department cannot utilize awarded Contracts to purchase from a bidder who cannot obtain an OAKS ID from Ohio Shared Services. In the event an awarded bidder is unable to obtain an OAKS ID, the Department shall reserve the right to revoke its award to the bidder and immediately cancel any resulting Contract.

A Supplier Information Form and W-9 must be completed and sent back directly to Ohio Shared Services in order to register and apply for an OAKS ID. The following website can be accessed by bidders to obtain both the forms and specific instructions for obtaining an OAKS ID:

http://ohiosharedservices.ohio.gov/SupplierOperations/Forms.aspx

It is strongly recommended that all interested bidders not already registered with Ohio Shared Services submit the above paperwork prior to the bid submission deadline.

2. **HOW BIDS MUST BE PackAGED**: All submitted bids in response to this procurement must be emailed to contracts.purchasing@dot.ohio.gov – Paper bids will NOT be accepted.

3. **WHAT NEEDS INCLUDED IN BID PACKAGE**: Submitted bid packages should include, at a minimum, a completed Signature Page, a completed Excel pricing page, and all necessary supportive documentation, forms, and any other information required herein. The Department may deem a bid non-responsive for failure to submit any of the documents requested above.

4. **PREBID QUESTIONS, DISCREPANCIES, AND CLARIFICATIONS**: Any discrepancies, omissions, ambiguities, or conflicts in or among the bidding documents or doubts as to the meaning shall be brought to the Department’s attention by the bidder no less than three (3) business days prior to the bid submission deadline. All questions, discrepancies, clarifications, etc. must be submitted electronically (hyperlink below). During the competitive bidding process, bidders (and their agents) are prohibited from contacting any ODOT office, including District offices, other than the Office of Contract Sales, Purchasing Services section to obtain responses to any questions. The Department may find a bidder non-responsive for failing to adhere to any of the above requirements.

Pre-bid questions/inquiries must be submitted electronically through the following website:

https://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Pages/PurchasePBQ1.aspx

Answers to Pre-Bid Questions/Inquiries will be posted on the following document available for download at the following website:

http://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Purchase/PBQ-Answers.doc

It is each bidder’s sole responsibility to check the website for updates to pre-bid questions and answers before submitting its bid package to the Department.

5. **MODIFICATIONS TO THE BIDDING DOCUMENTS**: When it is deemed necessary to modify these bidding documents, the Department will only do so by written addendum. The issuance of an addendum is dependent upon the information received and the impact on the competitive bid process. All issued addenda will be posted to the Department’s Upcoming ITB’s website and shall be automatically incorporated into the bidding/contract documents:

http://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/Lists/PurchaseUpcomingITBs/UpITBs.aspx

In addition to posting on the above website, the Department also may email addenda information out to all known bidders for convenience purposes only. The Department shall not be held responsible for a bidder’s
failure to receive the email with the addenda information. It is the sole responsibility of all interested bidders
to diligently visit the above-listed website to see if any addenda have been issued prior to submitting their
bid to the Department. Those interested in obtaining addenda information via email for a particular
procurement must send the Department its request in writing to the following email address:
Contracts.Purchasing@dot.ohio.gov

6. **PRE-BID CONFERENCES**: The Department reserves the right to hold mandatory or optional pre-bid
conferences at its discretion. Conferences may be held either in-person or via webinar/phone conference
formats. Bidders will be required to sign-in at all pre-bid conferences. The sign-in sheet for all pre-bid
conferences is considered a public record, will be kept in the bid file, and will be shared with any requesting
party. Additionally, any business cards collected during any pre-bid conference shall be considered public
records and may be distributed out to all conference attendees. Any changes to the requirements or
specifications of a procurement, as a result of the pre-bid conference content, will be made by written
addendum and publicly posted.

For mandatory pre-bid conferences, the Department requires that those companies intending on submitting
a bid be in attendance for the entire duration of the pre-bid conference. Mandatory pre-bid conferences will
officially begin five (5) minutes after the scheduled date and start time at the location specified in the
Special Terms and Conditions. Those bidders not in attendance at that time will be considered ineligible to
submit a bid. The conference will be considered adjourned and complete when a representative of the
Office of Contract Sales, Purchasing Services section indicates so. To be considered in attendance and
eligible to bid, a bidder must have at least one representative of the company in attendance. A single
representative cannot be present on behalf of two or more companies (bidders). Each company (bidder)
must send its own representative on behalf of their organization. It is the sole responsibility of the bidder to
ensure that the representative follows the sign-in procedures to properly document the bidder’s attendance.
The Department shall not be held responsible for a bidder’s failure to arrive at the meeting on time, properly
sign-in, or failure to stay for the entire duration of the meeting.

7. **WHERE BIDS MUST BE DELIVERED TO**: contracts.purchasing@dot.ohio.gov - Paper bids will NOT be
accepted.

8. **LATE BIDS**: A bid received after 1:00 p.m. eastern time, on the bid submission deadline (bid opening date)
established, shall be deemed “Late” and will not be considered for award of this procurement. The late bid
package will be marked as late, remain sealed, and will be kept in the Department’s bid file to serve as
official record of a late bid having been received.

Note: The Office of Contract Sales, Purchasing Services timeclock takes precedence over any other
timekeeping device (e.g. cell phones, other ODOT clocks, wrist watches, etc.) and will be utilized by the
Department to determine whether or not a bid was received by the 1:00 p.m. deadline.

9. **BID OPENING PROCEDURE**: Bids will usually be available within a day of the bid opening. Vendors can
submit requests for the bid tab to contracts.purchasing@dot.ohio.gov.

10. **BIDS FIRM**: Once opened, all bids are firm and cannot be altered by the bidder. Once a Contract is
awarded and executed, the Vendor shall deliver all products and/or services at the bid prices and terms
contained in the Contract. All submitted bids shall remain valid for a period of sixty (60) calendar days after
the date of the public bid opening. Beyond sixty (60) calendar days, bidders will have the option to either
honor their submitted bid or make a written request to withdraw their bid from consideration. The Ohio
Department of Transportation shall receive the benefit of any decrease in price during the sixty (60) day
period.

11. **WITHDRAWAL OF BIDS**: A bidder may, by way of written notice to the Purchasing Services section,
request to withdraw their bid response prior to the bid submission deadline. The request must be received
by the Purchasing Services Section PRIOR to the start of the public bid opening (beginning at 1:01 p.m.)
on the date of the bid submission deadline. Such written notice must set forth the specific reasons for the
bid withdrawal.

For requests to withdrawal a bid after the bid opening has begun, the bidder may request to withdraw their
bid response from consideration if the unit bid price(s) submitted are unreasonably lower than the other
bids received, provided the bid was submitted in good faith, and the reason for the unit bid price(s) being
substantially lower was due to an unintentional and substantial arithmetical error or unintentional omission
of a substantial quantity of material or labor in the compilation of the bid. Written notice of any such request to withdraw after the bid opening must be received by the Purchasing Services section within no later than forty-eight (48) hours of the scheduled bid opening.

The decision to allow a bid to be withdrawn is at the sole discretion of the Purchasing Services section. If the bid is to be awarded by category, lot, or group the withdrawal request will apply to all items within the category, lot, or group. All documents and conversations relating to any withdrawal request will become a part of the permanent bid file.

12. MODIFICATION OF SUBMITTED BIDS PRIOR TO BID OPENING: A bidder may request to modify their bid response prior to the scheduled date and time set for the public bid opening (i.e. bid submission deadline). To modify a bid response, the bidder must provide an alternate, complete bid package containing all required forms and necessary documents. The alternate bid package must have in the email subject line “REVISED”.

13. UNIT BID PRICES: The unit bid price(s) submitted shall govern the award of this procurement unless otherwise specified in the bid evaluation criteria. The unit bid price should be entered for each required bid item on the Department’s pricing page. Use of ditto marks, arrows, or other markings in lieu of the actual unit price may result in a non-responsive bid determination. Lot or group prices listed in the unit bid price area shall be considered as the unit price unless clearly identified as the lot price. Unless specifically allowed in the contract’s terms and conditions, requests to change or alter unit bid prices after the public bid opening are prohibited.

The following requirements also apply to unit bid prices:

a. DECIMAL POINT: Bidders should not insert a unit cost of more than two (2) digits to the right of the decimal point. Digit(s) beyond two (2) will be dropped and not recognized by the Department for the purposes of bid evaluation or contract award.

b. CREDIT CARD FEES: Bidders must incorporate into their unit bid price(s) submitted all costs and fees associated with the State’s use of a payment (credit) card.

c. DISCOUNTS: While bidders may offer to the Department discounts for prompt payment and other similar incentives, discounts and incentives these will not be used to alter the submitted unit bid price(s) for purposes of bid evaluation and contract award. This section only applies to bids awarded to the lowest responsive and responsible bidder either by individual bid item or group of bid items and does not include bids which are awarded to all responsive and responsible bidders (i.e. Multiple Award Contracts).

d. MULTIPLE AWARD CONTRACTS: Pursuant to Ohio Revised Code 5513.02, the Department may award Contracts to all responsive and responsible bidders for articles (i.e. bid items) meeting the general specifications provided. These are referenced by the Department as ‘Multiple Award Contracts’. Unit bid prices submitted for Multiple Award Contracts shall be considered by the Department as an amount-not-to-exceed unit bid price for the entire duration of the Contract. These awarded, amount-not-to-exceed bid prices often do not reflect potential quantity discounts, freight discounts, nor other similar discounts/incentives offered periodically by a distributor, manufacturer, or supplier. Where like or similar bid items are being offered by two or more awarded Vendors (bidders) on the awarded Contract, the Department reserves the right to obtain quotes from all awarded bidders on the Contract in order to achieve the best and most up-to-date pricing available to the Department at the time of ordering.

e. UNBALANCED BIDS: The Department will not accept unit bid prices that are deemed to be either materially or mathematically unbalanced. The final determination of an unbalanced unit bid price shall be at the Department’s sole discretion.

f. TIE BID PROCESS: If two or more responsive bids offer the same unit bid price, ODOT may break the tie as follows: during the bid evaluation process, the bidders that submitted tie bids will be contacted and given up to three (3) business days to submit a written revised unit price for the affected item or items. Bidders are not required to submit a revised unit price. In the event a tie still exists after the above-prescribed deadline has passed, ODOT will schedule a coin flip to be
conducted in the presence of both bidders. The winner of the coin flip will be deemed awarded the affected bid item(s).

14. **PREFERENCE FOR OHIO/BORDER STATE PRODUCTS**: The bid award for this procurement may be subject to the domestic preference provisions of the Buy America Act, 41 U.S.C.A., 10a-10d, as amended, and to the preference for Ohio products under O.R.C. Sections 125.09 and 125.11 and Ohio Administrative Code Rule 123:5-1-06. A bidder must complete the enclosed Ohio Bid Preference Certification Statement form to be eligible to receive any applicable bid preferences.

15. **RESPONSIVE BIDDER**: A bidder is responsive if its bid responds to the bid specifications in all material respects and contains no irregularities or deviations from the specifications that would affect the amount of the bid or otherwise give the bidder an unfair competitive advantage.

16. **MINOR INFORMALITIES OR IRREGULARITIES IN BIDS**: A minor informality or irregularity is one that is merely a matter of form and not of substance. It also pertains to some immaterial defect in a bid or variation of a bid from the exact requirements of the invitation that can be corrected or waived without being prejudicial to other bidders. The defect or variation is immaterial when the effect on price, quantity, quality, or delivery is negligible when contrasted with the total cost or scope of the supplies or services being acquired. The Department either shall give the bidder an opportunity to cure any deficiency resulting from a minor informality or irregularity in a bid or waive the deficiency, whichever is to the advantage of the Department.

17. **BIDDER RESPONSIBILITY**: The Department will only award this procurement to what it deems to be a responsible bidder. The Department’s determination of a bidder’s responsibility includes, but is not limited to, the following factors:

   a) experience of the bidder;
   b) bidder’s financial condition;
   c) bidder’s conduct and performance on previous contracts;
   d) the bidder’s facilities;
   e) the bidder’s management skills;
   f) the bidder’s employees;
   g) past experience and/or quality of bidder’s proposed subcontractors;
   h) the bidder’s ability to execute the contract;
   i) review of Federal and Department debarment lists;
   j) bidder has history of successful performance on contracts of similar size and scope; and
   k) current or impending legal actions against a bidder.

18. **APPARENT CLERICAL MISTAKES**: Clerical mistakes apparent on the face of the bid may be corrected, at the Department’s discretion, before contract award. The Department first shall obtain from the bidder a verification of the information intended and will attach written verification of the mistake by the bidder in the contract file and award documents. Example of apparent clerical mistakes are:

   (1) Obvious misplacement of a decimal point or comma;
   (2) Obvious incorrect discount factor; or
   (3) Transcription error in Part Number.

19. **ADDITIONAL INFORMATION**: The Department reserves the right to request additional information to evaluate a bidder’s responsiveness to the procurement’s requirements and/or to evaluate a bidder’s overall responsibility. These requests may require the bidder’s submission of confidential materials (e.g. financial statements). If a bidder does not provide all of the requested information within the prescribed timeframe, the Department may find the bid non-responsive and ineligible for award.

20. **PRODUCT SAMPLES**: The Department may require bidders, by procurement or by request during bid evaluation, to provide sample supplies or equipment or examples of work, at the Bidder’s expense. Samples must clearly identify the Bidder, the bid number, and the item the sample represents in the bid. The Department will return samples that are not destroyed by testing, at the Bidder's expense, upon the Bidder’s timely request. The Department may keep the samples of the Bidder awarded the contract until the completion of the contract. Unsolicited samples submitted in response to this procurement will not be evaluated and the Department may dispose of them in any way it chooses.
21. **SPECIFICATIONS:** The Department is authorized by Sections 5513 and/or 125.02(B) of the Ohio Revised Code to prepare specifications and establish contracts to obtain the supplies, equipment, and/or services referenced within this procurement. The purpose of the provided specifications is to describe the supplies, equipment, and/or services to be purchased and will serve as a fair and equitable basis for comparison of submitted bids. The Department may use any form of specification it determines to be in the best interest of the Department and that best describes the supplies or services to be purchased. Specifications may be in the form of a design specification or a combination thereof. If the department determines that a design, performance or a combination specification is not in the best interest of the Department, it may use brand name or equal specifications.

Unless otherwise specified in this procurement, all products, equipment, supplies, etc. offered by bidders must be in a new condition. A 'new' product is one that will be first used by the Department after it has been manufactured or produced. Used, reconditioned, or previously titled products, supplies, or equipment will not be considered for award of this procurement.

The Department uses qualified products list (QPL) and/or approved products lists (APL) developed by either itself or other qualified institutions to specify acceptable products and supplies that have been through proper application and testing procedures to verify conformance with technical and/or performance specifications. Where the Department requires products and supplies to be included on a specific QPL/APL listing, the Department will not accept bids for products/supplies that are not included on a specified QPL/APL at the time of public bid opening.

A bidder may not be compensated for damages arising from inaccurate or incomplete information in the procurement specifications or from inaccurate assumptions based upon the specifications.

22. **USE OF BRAND NAMES:** Unless otherwise provided in this solicitation, the name of a certain brand, make, or manufacturer does not restrict bidders to the specific brand, make, or manufacturer named, but conveys the general style, type, character, and quality of the article desired. Any article which the Department, in its sole discretion, determines to be the equivalent of that specified, considering quality, workmanship, economy of operation, or suitability for the purpose intended, may be accepted. The bidder is responsible to clearly and specifically identify the product being offered and to provide sufficient descriptive literature, catalog cuts and technical detail to enable the Department to determine if the product offered meets the requirements of the solicitation. Failure to furnish adequate data for evaluation purposes may result in declaring a bid nonresponsive. Unless the bidder clearly indicates in its bid that the product being offered is an equivalent product, such bid will be considered to offer the exact brand, make, or manufacturer name referenced in the bid solicitation.

23. **DEVIATIONS:** Statements or modifications made by a bidder in their submitted bid package that deviate from this procurement’s terms, conditions, specifications and requirements may render a bid non-responsive and ineligible for award.

Acceptance of any deviations or modifications will be confirmed by the Department in writing, if accepted. If the Department does not specifically approve submitted deviations or modifications in writing, an award of this procurement shall not constitute acceptance of the bidder’s submitted modifications.

24. **ESTIMATED QUANTITIES:** Any purchase estimates indicated for bid item(s) are to be considered as estimates only. The Department makes no representation or guarantee as to the actual amount of item(s) to be purchased by the Department or Political Subdivisions.

25. **OVERLAPPING CONTRACT ITEMS:** The products and/or services included in this solicitation may be available from other State of Ohio contracts and/or other contracts made available for the Department’s use. The existence of these contracts containing like or similar products and/or services could be either known or unknown to the Department at the time this procurement has been published. Unless otherwise stated in this contract, the Department may acquire these products and/or services from any available source. The Department will make purchases from sources that are deemed to be in the best interest of the Agency.

26. **REJECTION/PARTIAL AWARD OF BIDS:** The Department reserves the right to reject any or all bid responses, award partial contracts, or choose to rebid when:
(1) Product, supplies and/or services are not in compliance with the requirements, specifications, and terms and conditions set forth in this procurement; or

(2) Pricing offered is determined to be excessive in comparison with existing market conditions, or exceeds the available funds of the Department; or

(3) Only one bid is received, and the Department cannot determine the reasonableness of the bid prices submitted; or

(4) It is determined that the award of any or all items would not be in the best interest of the Department; or

(5) The Department, in its opinion, did not achieve the desired amount of competition amongst qualified bidders for the products, supplies, and/or services being offered in the bid solicitation; or

(6) Inadequate or ambiguous specifications were cited in the bidding documents; or

(7) The Department determines that specifications and/or requirements were missing from the bidding documents; or

(8) A bidder imposes additional terms and conditions against the Department.

27. **NOTICE TO BIDDERS OF REJECTED BIDS:** When the Department deems it necessary to reject a bid, the Department will notify each affected bidder and the reasons for such actions.

28. **BID PROTESTS:** Any apparent low bidder either deemed not responsible or whose bid has been deemed non-responsive shall be notified by the Department of that determination and the reasons for it. The notification will be provided by the Department in writing and sent by U.S. mail and at the email address provided on the front cover of the bidder’s bid. The bidder will have five (5) calendar days after receipt (by mail or email confirmation) of this notification to file a written, valid protest of the Department’s determination. A valid written protest must contain substantive information and evidence so as to refute the Department’s asserted claims against either the bid’s responsiveness or bidder’s responsibility, whichever apply. The Department will only review and respond to valid written protests containing substantive information and evidence. After review of the valid written protest, the Department will either affirm or reverse its original determination.

If a valid written protest is not received by the Department within five (5) calendar days of receipt, the Director of ODOT will move forward awarding the Contract and the affected bidder will have effectively waived its right to protest the Department’s decision. For the purposes of this paragraph, “receipt” shall be defined as verification (via either certified mail return receipt or electronic read or delivery receipt) that the apparent low bidder has received the Department’s written determination against the affected bidder. Upon the bidder’s receipt, the five (5) calendar day response deadline shall commence.

29. **DELAYS IN CONTRACT AWARD:** Delays in the award of this procurement beyond the anticipated Contract start date may result in a change in the contract period as indicated in the Special terms and conditions of this bid solicitation. In these instances, ODOT shall reserve the right to award a contract covering a period equal to or less than the initial contract term than originally specified in this bid solicitation.

30. **CONTRACT AWARD AND FORMATION:** Successful bidder(s) will receive via U.S. regular mail and/or email a Notice of Contract Award letter as well as a photocopy version of the Signature Page executed by both Parties. These documents shall serve to form the Contract between the Parties. The Signature Page must be executed by both the bidder and the Director of ODOT for the Contract to be deemed valid and enforceable. The Department will maintain in the Contract file the Signature Page document containing each parties’ original signature(s).

Upon award of a procurement, the bid invitation number (e.g. Invitation No. 999-16) will subsequently become the number assigned to the resulting Contract (e.g. ODOT Contract number 999-16) and will be referenced by the Department in all matters and documents related to said Contract.
Upon award of a procurement, successful bidders will thereafter be referenced as “Vendor” or “Contractor” by the Department in all matters and documents related to the resulting Contract.

31. **PUBLIC POSTING OF AWARDED CONTRACTS**: All Contracts awarded by the Office of Contract Sales, Purchasing Services section are posted to the Department’s website and open for public review. Successful bidders and awarded Contract pricing can be found by viewing the Contract’s award tab (Excel file). Award tabs can be accessed via the following website:


32. **PUBLIC RECORD**: All opened bids and their contents are subject to the Public Records Law, Section 149.43 of the Ohio Revised Code. Copies of bid responses must be requested and will be provided within a reasonable period of time and at a fee established by the Director of ODOT. To expedite and properly respond to such public records requests, a written request must be submitted to the Department. To prevent delays in evaluating bids and awarding contracts, such requests for recently opened bids, will be honored after a Contract has been executed.

   Bidders may request that specific information, such as trade secrets or proprietary data, be designated as confidential and not considered as public record. Material so designated shall accompany the bid and be in a sealed container duly marked, and shall be readily separable from the bid in order to facilitate public inspection of non-confidential portion. Prices, makes, models, catalog numbers of items offered, deliveries and terms of payment cannot be considered as confidential. The decision as to whether or not such trade secrets or proprietary data shall be disclosed at the bid opening rests solely with the Department.

   Requests to view previously submitted bids must be submitted in writing to either of the following addresses:

   [Contracts.Purchasing@dot.ohio.gov](mailto:Contracts.Purchasing@dot.ohio.gov)
   Ohio Department of Transportation
   Office of Contract Sales, Purchasing Services
   1980 West Broad St. Mail Stop 4110
   Columbus, OH 43223

   (the remainder of this page has been left intentionally blank)
General Definitions

(Last revised 11/30/2020)

When used in this procurement or any ensuing contract, the following definitions shall apply. If a conflict exists between these definitions and any definition listed in the bid specifications, the bid specifications shall prevail.

1. **Agency:** Ohio Department of Transportation.

2. **Authorized Distributor:** The bidder/vendor who maintains written legal agreements with manufacturers/producers to act as their agent and provide supplies, materials, equipment or services listed in the bid/contract. The authorized distributor must maintain active and sufficient facilities necessary to perform the awarded contract, own title to the goods inventoried within these facilities and maintain a true stock of these goods on a continuing basis and in sufficient quantity to provide uninterrupted service to ordering agencies.

3. **Bidder:** The company and/or authorized representative of the company who has signed and is submitting a bid response and who will be responsible to ensure proper performance of the contract awarded pursuant to the bid. The term bidder, proposer, contractor, or vendor may be used interchangeably in this document.

4. **Department:** Ohio Department of Transportation

5. **Equipment:** Items, implements and machinery with a predetermined and considerable usage life.

6. **F.O.B. Place of Destination:** Meaning the Vendor pays, and includes the cost of such in their bid, and bears the risk for the transportation/delivery of goods delivered to the specified locations provided by the Purchaser.

7. **Procurement/Contract:** All documents, whether attached or incorporated by reference, utilized for soliciting bids. Upon completion of the evaluation and award of the bidder's response, the procurement then becomes the contract between ODOT and the successful bidder, both governed by the laws of the State of Ohio.

8. **Invoice:** An itemized listing showing delivery of the commodity or performance of the service described in the order, and the date of the purchase or rendering of the service, or an itemization of the things done, material supplied, or labor furnished, and the sum due pursuant to the contract or obligation.

9. **Lowest Responsive/Responsible Bidder:** A bidder who offers the lowest cost for the goods or services listed in the bid; and whose proposal responds to bid specifications in all material respects and contains no irregularities or deviations from the specifications which would affect the amount of the bid or otherwise give him a competitive advantage; and whose experience, financial condition, conduct and performance on previous contracts, facilities, management skills evidences their ability to execute the contract properly.

10. **Minority Business Enterprise (MBE):** means an individual, partnership, corporation or joint venture of any kind that is owned and controlled by U.S. Citizens and residents of Ohio, who are and have held themselves out as members of the following socially and economically disadvantaged groups. Only businesses certified by the State of Ohio Equal Opportunity Division in accordance with Section 123.151 of the Ohio Revised Code shall be recognized as being MBE certified within the purpose of this invitation.

11. **Materials:** Items or substance of an expendable or non-expendable nature from which something can be made, improved or repaired.
13. PURCHASE: To buy, purchase, installment purchase, rent, lease, lease purchase or otherwise acquire equipment, materials, supplies or services. “Purchase” also includes all functions that pertain to obtaining of equipment, materials, supplies or services, including description of requirements, selection and solicitation of sources, preparation and award of contracts, and all phases of contract administration.

14. SERVICES: The furnishing of labor, time or effort by a person, not involving the delivery of a specific end product other than a report which, if provided, is merely incidental to the required performance. “Services” does not include services furnished pursuant to employment agreements or collective bargaining agreements.

15. SPECIFICATION: Any description of the physical or functional characteristics or of the nature of supplies, equipment, service, or insurance. It may include a description of any requirements for inspecting, testing, or preparing supplies, equipment, services, or insurance.

16. SUPPLIES: Provisions and items normally considered expendable or consumable.

17. UNBALANCED: Any unit price contained in the bid schedule which is obviously unbalanced either above or below reasonable cost analysis and or unreasonably disproportionate to current market prices as determined by the Director of ODOT, or if such unbalanced prices are contrary to the interest of the department.

18. VENDOR: The bidder who, upon awarding of a contract, then becomes a Vendor who is considered to be a primary source for providing the goods and/or services included in the awarded contract and the party to whom payment will be made upon delivery of the goods and/or completion of the contract.

19. SUBVENDOR/SUBCONTRACTOR: An individual, firm or corporation to whom the Vendor sublets part of the contract to be performed.

(the remainder of this page has been left intentionally blank)
1. **HEADINGS**: The headings used in this Contract are for convenience only and shall not be used to affect the interpretation of any of the Contract terms and conditions.

2. **ENTIRE CONTRACT**: This Contract consists of the complete procurement, including the Instructions, Terms and Conditions for Bidding, these Standard Contract Terms and Conditions, the Special Contract Terms and Conditions, ODOT Cooperative Purchasing Program Requirements, mutually executed Signature Page, Specifications and Requirements, awarded unit bid pricing, and any written addenda to the procurement; the completed competitive sealed bid, including proper modifications, clarifications and samples; and applicable, valid State of Ohio purchase orders or other ordering documents ("Contract").

3. **APPROPRIATION OF FUNDS**: Pursuant to the Constitution of the State of Ohio, Article II Section 22, ODOT's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the Ohio General Assembly fails at any time to continue funding for the payments or obligations due hereunder, the Work under this Contract that is affected by the lack of funding will terminate and ODOT will have no further obligation to make any payments and will be released from its obligations on the date funding expires.

   The current Ohio General Assembly cannot commit a future Ohio General Assembly to a future expenditure. If the term of this Contract extends beyond a biennium, the Contract will expire at the end of a current biennium and the State may renew this Contract in the next biennium by issuing written notice to the Vendor no later than July 1 of the new biennium. The operating biennium expires June 30th of each odd-numbered calendar year.

4. **OBM CERTIFICATION**: None of the rights, duties, or obligations in this Contract will be binding on the Department, and the Vendor will not begin its performance, until all of the following conditions have been met:
   1. All statutory provisions under the O.R.C., including Section 126.07, have been met; and
   2. All necessary funds are made available by the Ohio Office of Budget and Management; or
   3. If ODOT is relying on Federal or third-party funds for this Contract the ODOT gives the Vendor written notice that such funds have been made available.

5. **CONTRACT MODIFICATIONS**: Amendments or modifications to this Contract must be executed in writing between the parties and signed by the Director of ODOT. Amendments or modifications to this Contract made between the Vendor and other Department personnel shall be void and unenforceable.

6. **CONTRACT CONSTRUCTION**: Any general rule of construction to the contrary notwithstanding this Contract shall be liberally construed in favor of the effect the purpose of this Contract and the policy and purposes of the Department. If any provisions in this Contract are found to be ambiguous, an interpretation consistent with the purpose of this Contract that would render the provision valid shall be favored over any interpretation that would render it invalid.

7. **GOVERNING LAW / SEVERABILITY**: This Contract shall be governed by the laws of the State of Ohio, and the venue for any disputes will be exclusively with the appropriate court in Franklin County, Ohio. If any provision of the Contract or the application of any provision is held by that court to be contrary to law, the remaining provisions of the Contract will remain in full force and effect.

8. **ASSIGNMENT / DELEGATION**: The Vendor will not assign any of its rights nor delegate any of its duties under this Contract without the written consent of the Director of ODOT. Any assignment or delegation not consented to may be deemed void by the Department.

9. **PLACEMENT OF ORDERS/METHODS OF PAYMENT**: The Department shall use either State of Ohio Purchase Order or State of Ohio Payment Card (i.e. credit card) to authorize performance under this Contract and to issue payments for supplies, products, and/or services acquired. Vendors are required to
accept both forms of payment. For Department purchases over $2,500.00, an official State of Ohio purchase order must be generated and obtain approvals from the Office of Budget and Management, the Department of Administrative Services, and the Director of Transportation prior to its effectiveness. An approved State of Ohio purchase order will be sent to the Vendor and the Vendor will provide the goods and/or services listed on the ordering documents and in accordance with the Contract's terms and conditions. Any order placed not using an approved ODOT purchase order or against a State payment card, shall not be considered a valid order and may result in denial of payment and/or return of goods at the Vendor's expense.

10. **ACCEPTANCE OF ORDERS**: The Vendor must accept orders placed by the Department pursuant to this Contract up through the last day of the Contract's effectiveness, inclusive of any contract extensions exercised or agreed-upon between the Parties.

11. **BLANKET PURCHASE ORDERS**: The Department utilizes blanket purchase orders to pre-authorize funding for use on Contracts containing bid items that, due to the urgent nature of maintaining the Department's highways and facilities, are critical to the Department executing its mission and objectives. The generation of blanket purchase orders are not used by the Department to place a specific order, rather as a means to make funding more readily available for use when Contract items are needed. The Vendor shall keep all blanket purchase orders on file and make them readily available for use by Department personnel to place orders against. When placing orders against a blanket purchase order, the Department will telephone or email orders referencing the blanket purchase order and its associated ODOT purchase order number. All of the Contract's terms and conditions shall apply to the Department's orders referencing a blanket purchase order.

For all blanket purchase orders, quantities and amounts to be purchased from these purchase orders is unknown by the Department and Vendors must not construe these purchase orders as a commitment to purchase a specific amount of goods and/or services. Accordingly, the Department reserves the right to increase or decrease the available funding on these blanket purchase orders at its discretion.

12. **DELIVERY INSPECTION AND ACCEPTANCE**: Upon pick-up or delivery of any supplies, products, and/or services, ODOT retains the right to inspect the product/service prior to final acceptance and/or payment for the product/service. ODOT shall have sufficient and reasonable time to fully inspect supplies and/or services for compliance. The purpose of the inspection process is to ensure that the product/service is in compliance with the specifications set forth in the awarded contract. In the event that the product/service does not meet the specifications, ODOT shall notify the Vendor for removal/replacement of the product and/or service at the Vendor's expense. ODOT shall retain all rights and remedies as described herein. Wherein products ordered by ODOT are delivered to a facility, which is not owned by ODOT and where ODOT has contracted with this facility to take delivery of products ordered by ODOT, acceptance will occur when the products have been inspected and accepted by ODOT within a reasonable amount of time after delivery to the facility. ODOT shall not be responsible for any storage costs incurred prior to the inspection and acceptance.

13. **RETURN GOODS POLICY**: The Department will apply the following Return Goods Policy on all purchases made under the Contract:

(A) Return goods, when due to Vendor debar (i.e. over-shipment, defective merchandise, unapproved substitution, etc.) shall be returned to the Vendor, at the Vendor’s expense. The Vendor shall make arrangements to remove the return goods from the Department’s premises within five (5) calendar days after notification. The Vendor shall not apply any restocking or other charges to the Department. At the option of the Department, replacement items may be accepted and will be shipped within five (5) calendar days of notification. Failure of the Vendor to arrange for return of the items within the specified time will result in the items being deemed as abandoned property and the Department will dispose of accordingly.
(B) For orders of custom manufactured items, the Vendor will provide a production sample of the item to the Department for acceptance. The production sample will be identical to the item to be provided. The Department will provide written acceptance of the item prior to the Vendor continuing with production. Once delivery and acceptance has been completed and the Department determines for any reason that any remaining quantities will not be used, the agency may request the return of the custom manufactured items. Acceptance of the return of custom manufactured items will be at the option of the Vendor. If the Vendor agrees to the return of these items, the Department will be responsible for all costs associated with packaging, shipment and transportation, to include the original shipment to the Department and subsequent return of goods to the location designated by the Vendor. The Vendor may assess restocking fees that are equivalent to restocking fees that are normally assessed to other customers or as published by the Vendor. Failure of the Vendor to provide a production sample and obtain written approval from the Department will result in the Vendor bearing all responsibility and costs associated with the return of these goods.

(C) Return goods of regular catalog stock merchandise, when due to Department error (i.e. over purchase, discontinued use, inventory reduction, etc.) will be accepted by the Vendor if notice is given by the Department within six (6) months of delivery and acceptance. All items to be returned must be unused and in their original containers and in suitable condition for resale. The Department will be responsible for all transportation costs associated with both the original shipment of items to the agency and the subsequent return of the items to the location designated by the Vendor. The Vendor may assess a restocking fee (not to exceed 10%) associated with the return of the items to the location designated by the Vendor. Return of regular stock catalog merchandise, when delivery and acceptance exceed six (6) months will be at the option of the Vendor.

14. **PRODUCT RECALLS:** In the event product delivered has been recalled, seized, or embargoed and/or has been determined to be misbranded, adulterated, or found to be unfit for human consumption by the packer, processor, manufacturer or by any Department or Federal regulatory agency, the Vendor shall be responsible to notify the ODOT Office of Contract Sales, Purchasing Services section and all other ordering agencies/entities within two business days after notice has been given. Vendor shall, at the option of the Department, either reimburse the purchase price or provide an equivalent replacement product at no additional cost. Vendor shall be responsible for removal and/or replacement of the affected product within a reasonable time as determined by the ordering agency. At the option of the ordering agency, Vendor may be required to reimburse storage and/or handling fees to be calculated from time of delivery and acceptance to actual removal. Vendor will bear all costs associated with the removal and proper disposal of the affected product. Failure to reimburse the purchase price or provide equivalent replacement product will be considered a default.

15. **PRODUCT SUBSTITUTION:** In the event a specified product listed in the Contract becomes unavailable or cannot be supplied by the Vendor for any reason (except as provided for in the Force Majeure clause), a product deemed in writing by the Department to be equal to or better than the specified product must be substituted by the Vendor at no additional cost or expense to the Department. Unless otherwise specified, any substitution of product prior to the Department’s written approval may be cause for termination of Contract.

The Department reserves the right to deny any substitution request that it is deemed to not be in the best interest of the Department. In these instances, the Department may seek substitute products from another supplier and assess the difference in cost, if any, as damages against the Vendor for their material breach.

16. **INVOICE REQUIREMENTS:** The Vendor must submit an original, proper invoice to the office designated on the purchase order as the “bill to” address. To be a proper invoice, the invoice must include the following information: 1. The ODOT purchase order number authorizing the delivery of products or services. 2. A description of what the Vendor delivered, including, as applicable, the time period, serial number, unit price, quantity, and total price of the products and services. 3. The Contract number pursuant to the deliverable.
17. **DEFECTIVE INVOICES**: In the event the Department is in receipt of defective or improper invoices, the Department shall postpone payment pursuant to Section 126.30 of the Ohio Revised Code. Invoices shall be returned to the Vendor noting areas for correction. If such notification of defect is sent, the required payment date shall be thirty (30) calendar days after receipt of the corrected invoice.

18. **PAYMENT DUE DATE**: Payments under this Contract will be due on the 30th calendar day after the date of actual receipt of a proper invoice in the office designated to receive the invoice, or the date the service is delivered and accepted in accordance with the terms of this Contract. The date of the warrant issued in payment will be considered the date payment is made. Interest on late payments will be paid in accordance with O.R.C. Section 126.30.

19. **INSURANCE POLICIES**: By way of provision in this Contract to maintain specific minimum levels of insurance coverage(s) (e.g. Commercial General liability, Auto liability, Public liability, Property Damage, etc.), the Vendor shall provide to Department upon request evidence of such insurance required to be carried by these provisions, including any endorsement affecting the additional insured status, is in full force and effect and that premiums therefore have been paid. Such evidence shall be furnished by the Vendor within two (2) business days and on the insurance industry's standard ACORD Form (Certificate of Insurance) or a certified copy of the original policy. The Certificate of Insurance or certified copy of the policy must contain an endorsement naming the State of Ohio, Department of Transportation, its officers, agents, employees, and servants as additionally insured, but only with respect to Work performed for the Department under this Contract, at no cost to Department. Vendor shall notify the Department within ten (10) calendar days of receipt of a notice of cancellation, expiration, or any reduction in coverage, or if the insurer commences proceedings or has proceedings commenced against it, indicating the insurer is insolvent. Vendor shall provide to the Department evidence of a replacement policy at least five (5) calendar days prior to the effective date of such cancellation, expiration, or reduction in coverage.

All required insurance policies shall be maintained at Vendor's sole expense and in full force for the complete term of the Contract, including any warranty periods. Reference 107.12 the Construction & Materials Specification handbook.

20. **TAXATION**: ODOT is exempt from federal excise taxes and all Department and local taxes, unless otherwise provided herein. ODOT does not agree to pay any taxes on commodities, goods, or services acquired from any Vendor.

21. **CONTRACT TERMINATION**: If a Vendor fails to perform any one of its obligations under this Contract, it will be in breach of contract and the Department may terminate this Contract in accordance with this section. Notices of contract termination shall be made in writing. The termination will be effective on the date delineated by the Department.

   a. **Termination for Breach**. If Vendor's breach is unable to be cured in a reasonable time, the Department may terminate the Contract by written notice to the Vendor.

   b. **Termination for Un-remedied Breach**. If Vendor's breach may be cured within a reasonable time, the Department will provide written notice to Vendor specifying the breach and the time within which Vendor must correct the breach. If Vendor fails to cure the specified breach within the time required, the Department may terminate the Contract. If the Department does not give timely notice of breach to Vendor, the Department has not waived any of the Department's rights or remedies concerning the breach.

   c. **Termination for Persistent Breach**. The Department may terminate this Contract by written notice to Vendor for defaults that are cured, but persistent. "Persistent" means three or more breaches. After the Department has noticed Vendor of its third breach, the Department may terminate this Contract without providing Vendor with an opportunity to cure. The three or more breaches are not required to be related to each other in any way.

   d. **Termination for Endangered Performance**. The Department may terminate this Contract by written notice to the Vendor if the Department determines that the performance of the Contract is endangered through no fault of the Department.
e. Termination for Financial Instability. The Department may terminate this Contract by written notice to the Vendor if a petition in bankruptcy or a Federal or State tax lien has been filed by or against the Vendor.

f. Termination for Delinquency, Violation of Law. The Department may terminate this Contract by written notice, if it determines that Vendor is delinquent in its payment of federal, Department or local taxes, workers’ compensation, insurance premiums, unemployment compensation contributions, child support, court costs or any other obligation owed to a Department agency or political subdivision. The Department also may cancel this Contract, if it determines that Vendor has violated any law during the performance of this Contract. However, the Department may not terminate this Contract if the Vendor has entered into a repayment agreement with which the Vendor is current.

g. Termination for Subcontractor Breach. The Department may terminate this Contract for the breach of the Vendor or any of its subcontractors. The Vendor will be solely responsible for satisfying any claims of its subcontractors for any suspension or termination and will indemnify the Department for any liability to them. Subcontractors will hold the Department harmless for any damage caused to them from a suspension or termination. The subcontractors will look solely to the Vendor for any compensation to which they may be entitled.

h. Termination for Vendor’s Failure to Pay Material Suppliers. Pursuant to Section 4113.61 of the Ohio Revised Code, Vendors shall promptly pay material suppliers, within ten (10) calendar days of receipt of payment from the State of Ohio, for materials ordered and delivered as a result of this contract. A Vendor unable to furnish bid items because of non-payment issues related to a material supplier shall constitute grounds for the Director of ODOT to terminate this contract immediately. A Vendor may, at the discretion of the Department, be given an amount of time, amount shall be specified by the Department in writing, to furnish past due payment to the material supplier before termination shall occur.

j. Failure to Maintain MBE Certification. Pursuant to O.R.C. Section 125.081, the State may set aside a bid for supplies or services for participation only by minority business enterprises (MBE’s) certified by the State of Ohio, Equal Opportunity Coordinator. After award of the Contract, it is the responsibility of the MBE Vendor to maintain certification as a MBE. If the Vendor fails to renew its certification and/or is decertified by the State of Ohio, Equal Opportunity Coordinator, the State may immediately cancel the Contract.

k. Failure to Maintain Licensure. The Vendor’s failure to maintain the proper license(s) to perform the services or provide the goods prescribed by this Contract shall be grounds to terminate this Contract without prior notice.

l. Qualified Products Listing and Approved Products Listing. Any products or supplies removed from a specific qualified products listing/approved product listing, by either the Department, government, or governing body throughout the duration of the Contract shall be removed from the Contract effective on the date of removal from the respective listing.

22. NOTICE OF BREACH: Each party of this Contract has an obligation to provide written notice when it is determined by one party that the other party is in default of this Contract. A notice of ODOT’s default of this Contract must be sent to the Procurement Manager of the ODOT Office of Contract Sales.

23. CONTRACT SUSPENSION: A Vendor who fails to perform any one of its obligations under this Contract will be in breach. In these instances, ODOT may choose to suspend the Vendor from the contract rather than terminate the Contract.

In the case of a suspension for ODOT’s convenience, the amount of compensation due the Vendor for work performed before the suspension will be determined in the same manner as provided in this section for termination for ODOT’s convenience or the Vendor may be entitled to compensation for work performed before the suspension, less any damage to ODOT resulting from the Vendor’s breach of this Contract or other fault.

The notice of suspension, whether with or without cause, will be effective immediately on the Vendor’s receipt of the notice. The Vendor will immediately prepare a report and deliver it to ODOT which will
include a detailed description of work completed, percentage of project completion, estimated time for
delivery of all orders received to date, and costs incurred by the Vendor.

24. **Termination for Convenience.** The Contracting Agency may terminate this Contract, or an Ordering
Agency may terminate an order placed under this Contract, for its convenience after issuing written notice
to the Contractor. The Contractor will be entitled to the pro-rated price for any Deliverable or portion of a
Deliverable that the Contractor has delivered and the Ordering Agency or the State has accepted before
the termination. Total payments will not exceed the amount payable to the Contractor as if the Contract or
order had been fully performed. This will be the Contractor’s exclusive remedy in the case of termination for
convenience and is available to the Contractor only after the Vendor has submitted an invoice that
complies with Section 16 of these Standard Contract Terms and Conditions.

25. **CONTRACT DAMAGES:** The Department may assess, at a minimum but not limited to, the following
damages against a Vendor:

A. **ACTUAL DAMAGES:** Vendor is liable to the State of Ohio for all actual and direct
damages caused by Vendor’s breach. The Department may substitute supplies or
services, from a third party, for those that were to be provided by Vendor. In accordance
with Ohio Revised Code §5513.05(c), the Department may recover the costs associated
with acquiring substitute supplies or services, less any expenses or costs saved by
Vendor’s breach, from Vendor.

B. **LIQUIDATED DAMAGES:** If actual and direct damages are uncertain or difficult to
determine, the Department may recover liquidated damages in the amount of 1% of the
value of the order, deliverable or milestone that is the subject of the breach for every day
that the breach is not cured by the Vendor. If Delay of the cure is caused by ODOT, the
delivery date shall be extended accordingly to offset such delays. Approval to extend any
scheduled delivery date(s) shall be at the sole discretion of ODOT.

C. **DEDUCTION OF DAMAGES FROM CONTRACT PRICE:** The Department may deduct all
or any part of the damages resulting from Vendor’s breach from any part of the price still
due on the contract, upon prior written notice issued to the Vendor by the Department.

D. **INCIDENTAL/CONSEQUENTIAL DAMAGES:** Pursuant to Section 5513.05 of the Ohio
Revised Code, the Department may recover from a Vendor who fails to promptly provide
conforming articles, any incidental or consequential damages as defined in Section
1302.89 of the Ohio Revised Code, incurred by the Department in promptly obtaining the
conforming articles.

26. **CONTRACT TERM EXTENSIONS:** ODOT reserves the right to unilaterally extend this Contract up to one
(1) calendar month beyond the original contract expiration date at the original unit bid prices awarded.
Contract extensions beyond one (1) calendar month shall be executed by means of written, mutual
agreement with the Contract Vendor, but in no instance with the Contract be extended beyond the
biennium unless it is procured as a multi-year contract stating an option for biennial extension.

27. **FIRM, FIXED PRICE CONTRACT:** Unless otherwise specified in the bidding documents, this Contract is a
Firm, Fixed-Price Contract. The Vendor will be required to provide to the Department with the materials,
supplies, equipment and/or services at the awarded bid price(s) for the entire duration of the contract, and
any extensions thereto.

28. **FORCE MAJEURE:** If the Department or Vendor is unable to perform any part of its obligations under this
Contract by reason of force majeure, the party will be excused from its obligations, to the extent that its
performance is prevented by force majeure, for the duration of the event. The party must remedy with all
reasonable dispatch the cause preventing it from carrying out its obligations under this Contract. The term
“force majeure” means without limitation: acts of God; such as epidemics; lightning; earthquakes; fires;
storms; hurricanes; tornadoes; floods; washouts; droughts; any other severe weather; explosions; restraint
of government and people; war; labor strikes; and other like events.

29. **EQUAL EMPLOYMENT OPPORTUNITY:** The Vendor will comply with all state and federal laws regarding
equal employment opportunity, including O.R.C. Section 125.111 and all related Executive Orders.
30. **ANTITRUST ASSIGNMENT TO THE DEPARTMENT**: Vendor assigns to the State of Ohio, through the Department of Transportation, all of its rights to any claims and causes of action the Vendor now has or may acquire under Department or federal antitrust laws if the claims or causes of action relate to the supplies or services provided under this Contract. Additionally, the State of Ohio will not pay excess charges resulting from antitrust violations by Vendor’s suppliers and subcontractors.

31. **CONFIDENTIALITY**: The Vendor may learn of information, documents, data, records, or other material that is confidential in the performance of this Contract. The Vendor may not disclose any information obtained by it as a result of this Contract, without the written permission of the Department. The Vendor must assume that all Department information, documents, data, records or other material is confidential.

The Vendor’s obligation to maintain the confidentiality of the information will not apply where it: (1) was already in the Vendor’s possession before disclosure by the Department, and it was received by the Vendor without the obligation of confidence; (2) is independently developed by the Vendor; (3) is or becomes publicly available without breach of this Contract; (4) is rightfully received by the Vendor from a third party without an obligation of confidence; (5) is disclosed by the Vendor with the written consent of the Department; or (6) is released in accordance with a valid order of a court or governmental agency, provided that the Vendor (a) notifies the Department of such order immediately upon receipt of the order and (b) makes a reasonable effort to obtain a protective order from the issuing court or agency limiting disclosure and use of the confidential information solely for the purposes intended to be serviced by the original order of production. The Vendor will return all originals of any information and destroy any copies it has made on termination or expiration of this Contract.

The Vendor will be liable for the disclosure of any confidential information. The parties agree that the disclosure of confidential information of the Department’s may cause the Department irreparable damage for which remedies other than injunctive relief may be inadequate, and the Vendor agrees that in the event of a breach of the obligations hereunder, the Department shall be entitled to temporary and permanent injunctive relief to enforce this provision without the necessity of providing actual damages. This provision shall not, however, diminish or alter any right to claim and recover.

32. **DRUG-FREE WORKPLACE**: The Vendor agrees to comply with all applicable Department and federal laws regarding drug-free workplace and shall make a good faith effort to ensure that all its employees, while working on Department property, will not purchase, transfer, use or possess illegal drugs or alcohol or abuse prescription drugs in any way.

33. **WORKERS’ COMPENSATION**: Workers’ compensation insurance, as required by Ohio law or the laws of any other Department where work under this Contract will be done. The Vendor will also maintain employer’s liability insurance with at least a $1,000,000.00 limit.

34. **OHIO ETHICS LAW**: Vendor agrees that it is currently in compliance and will continue to adhere to the requirements of Ohio Ethics law as provided by Section 102.03 and 102.04 of the Ohio Revised Code.

35. **PUBLICITY**: The Vendor will not advertise that it is doing business with the Department or use this Contract as a marketing or sales tool without prior, written consent of the Department. This provision includes marketing or sales tools related to the ODOT Cooperative Purchasing Program.

36. **STRICT PERFORMANCE**: The failure of either party, at any time to demand strict performance by the other party of any of the terms of this Contract, will not be construed as a waiver of any such term and either party may at any time demand strict and complete performance by the other party.

37. **SUBCONTRACTING**: The Department recognizes that it may be necessary for the Vendor to use subcontractors to perform portions of the work under the Contract. In those circumstances, the Vendor shall submit a list identifying its subcontractors or joint venture partners performing portions of the work under the Contract. If any changes occur during the term of the Contract, the Vendor shall supplement its list of subcontractors or joint venture business partners. In addition, all subcontractors or joint venture business partners agree to be bound by all of the Terms and Conditions and specifications of the Contract. The Department reserves the right to reject any subcontractor submitted by the Vendor. All subcontracts will be at the sole expense of the Vendor and the Vendor will be solely responsible for payment of its subcontractors. The Vendor assumes responsibility for all sub-contracting and third party manufacturer work performed under the Contract. In addition, Vendor will cause all subcontractors to be bound by all of
the Terms and Conditions and specifications of the Contract. The Vendor will be the sole point of contact with regard to all contractual matters.

38. **SURVIVORSHIP**: All sections herein relating to payment, confidentiality, license and ownership, indemnification, publicity, construction warranties, limitations of warranties and limitations on damages shall survive the termination of this Contract.

39. **GENERAL REPRESENTATIONS AND WARRANTIES**: The Vendor warrants that the recommendations, guidance, and performance of the Vendor under this Contract will:

   1. Be in accordance with the sound professional standards and the requirements of this Contract and without any material defect.

   2. No services, products or supplies will infringe on the intellectual property rights of any third party.

   3. All warranties are in accordance with Vendor’s standard business practices attached.

   4. That the products or supplies hereunder are merchantable and fit for the particular purpose described in this contract. Additionally, with respect to the Vendor’s activities under this Contract, the Vendor warrants that:

   5. The Vendor has the right to enter into this Contract.

   6. The Vendor has not entered into any other contracts or employment relationships that restrict the Vendor’s ability to perform under this Contract.

   7. The Vendor will observe and abide by all applicable laws and regulations, including those of the Department regarding conduct on any premises under the Department’s control.

   8. The Vendor has good and marketable title to any products or supplies delivered under this Contract and which title passes to the Department.

   9. The Vendor has the right and ability to grant the license granted in products or supplies in which title does not pass to the Department. If any services of the Vendor or any products or supplies fails to comply with these warranties, and the Vendor is so notified in writing, the Vendor will correct such failure with all due speed or will refund the amount of the compensation paid for the services, products or supplies. The Vendor will also indemnify the Department for any direct damages and claims by third parties based on breach of these warranties.

40. **VENDOR’S WARRANTY AGAINST AN UNRESOLVED FINDING FOR RECOVERY**: Vendor warrants that it is not subject to an unresolved finding for recovery under O.R.C. Section 9.24. If the warranty was false on the date the parties signed this Contract, the Contract is void ab initio.

41. **LIMITATION OF LIABILITY**: Notwithstanding any limitation provisions contained in the documents and materials incorporated by reference into this contract, the Vendor agrees that the Vendor shall be liable for all direct damages due to the fault or negligence of the Vendor.

42. **INDEMNITY**: The Vendor will indemnify the Department for any and all claims, damages, lawsuits, costs, judgments, expenses, and any other liabilities resulting from bodily injury to any person (including injury resulting in death) or damage to property that may arise out of or are related to Vendor’s performance under this Contract, providing such bodily injury or property damage is due to the negligence of the Vendor, its employees, agents, or subcontractors. Reference 107.12 the Construction & Materials Specification handbook, if applicable for this product or service.

   The Vendor will also indemnify the Department against any claim of infringement of a copyright, patent, trade secret, or similar intellectual property rights based on the Department’s proper use of any products or supplies under this Contract. This obligation of indemnification will not apply where the Department has modified or misused the products or supplies and the claim of infringement, is based on the modification or misuse. The Department agrees to give the Vendor notice of any such claim as soon as reasonably practicable and to give the Vendor the authority to settle or otherwise defend any such claim upon consultation with and approval by the Office of the Department Attorney General. If a successful claim of
infringement is made, or if the Vendor reasonably believes that an infringement claim that is pending may actually succeed, the Vendor will take one (1) of the following four (4) actions:

1. Modify the products or supplies so that is no longer infringing;
2. Replace products or supplies with an equivalent or better item;
3. Acquire the right for the Department to use the infringing products or supplies as it was intended for the Department to use under this Contract; or
4. Remove the products or supplies and refund the fee the Department paid for the products or supplies and the fee for any other products or supplies that required the availability of the infringing products or supplies for it to be useful to the Department.

43. **AUDITS**: The Vendor must keep all financial records in a manner consistent with generally accepted accounting principles. Additionally, the Vendor must keep separate business records for this Contract, including records of disbursements and obligations incurred that must be supported by contracts, invoices, vouchers and other data as appropriate. During the period covered by this Contract and until the expiration of three (3) years after final payment under this Contract, the Vendor agrees to provide the Department, its duly authorized representatives or any person, agency or instrumentality providing financial support to the work undertaken hereunder, with access to and the right to examine any books, documents, papers and records of the Vendor involving transactions related to this Contract. The Vendor shall, for each subcontract in excess of two thousand five hundred ($2,500), require its subcontractor to agree to the same provisions of this Article. The Vendor may not artificially divide contracts with its subcontractors to avoid requiring subcontractors to agree to this provision. The Vendor must provide access to the requested records no later than (5) five business days after the request by the Department or any party with audit rights. If an audit reveals any material deviation from the Contract requirements, and misrepresentations or any overcharge to the Department or any other provider of funds for the Contract, the Department or other party will be entitled to recover damages, as well as the cost of the audit.

44. **INDEPENDENT CONTRACTOR ACKNOWLEDGEMENT**: It is fully understood and agreed that Vendor is an independent contractor and is not an agent, servant, or employee of the State of Ohio or the Ohio Department of Transportation. Vendor declares that it is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including but not limited to any insurance coverage, workers’ compensation, or unemployment compensation that is required in the normal course of business and will assume all responsibility for any federal, state, municipal or other tax liabilities. Additionally, Vendor understands that as an independent contractor, it is not a public employee and is not entitled to contributions from the State to any public employee retirement system.

**TRADE**: Pursuant to R.C. 9.76(B), Vendor warrants that Vendor is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the term of this Contract.

45. **EXECUTIVE ORDER 2019-12D**: The Vendor affirms to have read and understands Executive Order 2019-12D issued by Ohio Governor Mike DeWine and shall abide by those requirements in the performance of this Contract, shall sign and require its subcontractors (if any) to sign the attached “Standard Affirmation and Disclosure Form,” and shall perform no services required under this Contract outside of the United Departments. The Executive Order is incorporated by reference and also is available at the following website: [https://procure.ohio.gov/pdf/EO2019-12D/Executive_Order_2019_12WEB.pdf](https://procure.ohio.gov/pdf/EO2019-12D/Executive_Order_2019_12WEB.pdf)

The Vendor also affirms, understands, and agrees to immediately notify the Department of any change or shift in the location(s) of services performed by the Vendor or its subcontractors under this Contract, and no services shall be changed or shifted to a location(s) that are outside of the United Departments.

46. **NON-DISCRIMINATION/COMPLIANCE WITH APPLICABLE LAWS**: Vendor agrees that Vendor, any subcontractor, and any person acting on behalf of Vendor or a subcontractor, shall not discriminate, by reason of race, color, religion, sex (including pregnancy, gender identification and sexual orientation), age (40 years or older), disability, military status, national origin, or ancestry against any citizen of this state in the employment of any person qualified and available to perform the Work. Vendor further agrees that Vendor, any subcontractor, and any person acting on behalf of Vendor or a subcontractor shall not, in any manner, discriminate against, intimidate, or retaliate against any employee hired for the performance of the Work on account of race, color, religion, sex (including
pregnancy, gender identification and sexual orientation), age, disability, military status, national origin, or ancestry.

During the performance of this Contract, the Vendor, for itself, its assignees, and successors in interest agrees to comply with the Federal Requirements as follows:

1. Vendor will ensure that applicants are hired and that employees are treated during employment without regard to their race, religion, color, sex (including pregnancy, gender identification and sexual orientation), national origin (ancestry), disability, genetic information, age (40 years or older), or military status (past, present, or future). Such action shall include, but not be limited to, the following: 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.

2. Vendor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause. Vendor will, in all solicitations or advertisements for employees placed by or on behalf of Vendor, state that all qualified applicants will receive consideration for employment without regard to race, religion, color, sex (including pregnancy, gender identification and sexual orientation), national origin (ancestry), disability, genetic information, age (40 years or older), or military status (past, present, or future).

3. Vendor agrees to fully comply with Title VI of the Civil Rights Act of 1964, 42 USC Sec. 2000. Vendor shall not discriminate on the basis of race, color, national origin, sex (including pregnancy, gender identification and sexual orientation), age, disability, low-income status, or limited English proficiency in its programs or activities. The Director of Transportation may monitor the Vendor’s compliance with Title VI.

4. Compliance with Regulations: The Vendor (hereinafter includes consultants) will comply with the Acts and Regulations relative to Non-discrimination in Federally-assisted programs of the U.S. Department of Transportation, Federal Highway Administration (FHWA), as they may be amended from time to time, which are herein incorporated by reference and made a part of this contract.

5. Nondiscrimination: The Vendor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, national origin (ancestry), sex (including pregnancy, gender identification and sexual orientation), age (40 years or older), disability, low-income status, or limited English proficiency in the selection and retention of subcontractors, including procurements of materials and leases of equipment. The Vendor will not participate directly or indirectly in the discrimination prohibited by the Acts and the Regulations as set forth in section 10. above, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR Part 21.

6. Solicitations for Subcontractors, including procurements of Materials and Equipment: In all solicitations, either by competitive bidding, or negotiation made by the Vendor 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 Vendor of the Vendor’s obligations under this contract and the Acts and the Regulations relative to nondiscrimination on the grounds of race, color, national origin (ancestry), sex (including pregnancy, gender identification and sexual orientation), age (40 years or older), disability, low-income status, or limited English proficiency.

7. Information and Reports: The Vendor 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 Ohio Department of Transportation (hereinafter “ODOT”) or FHWA to be pertinent to ascertain compliance with such Acts, Regulations, and instructions. Where any information required of a Vendor is in the exclusive possession of another who fails or refuses to furnish this information, the Vendor will so certify to ODOT or FHWA, as appropriate, and will set forth what efforts it has made to obtain the information.
8. Sanctions for Noncompliance: In the event of the Vendor’s noncompliance with the nondiscrimination provisions of this contract, ODOT will impose such contract sanctions as it or FHWA may determine to be appropriate, including, but not limited to:

   a. Withholding of payments to the Vendor under the contract until the Vendor complies, and/or
   b. Cancellation, termination or suspension of the contract, in whole or in part.

9. Incorporation of Provisions: The Vendor will include the provisions of sections 1. through 9. in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations, and directives issued pursuant thereto. The Vendor will take action with respect to any subcontract or procurement as ODOT or FHWA may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the Vendor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the Vendor may request ODOT to enter into any litigation to protect the interests of ODOT. In addition, the Vendor may request the United States to enter into the litigation to protect the interests of the United States.

10. During the performance of this contract, the Vendor, for itself, its assignees, and successors in interest, consultants and sub-contractors, agrees to comply with the following non-discrimination statutes and authorities; including but not limited to:

**Pertinent Non-Discrimination Authorities:**

- 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
- 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)
- 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
- The Age Discrimination Act of 1975, as amended (42 U.S.C. § 6101 et seq.) (prohibits discrimination on the basis of age)
- Airport and Airway Improvement Act of 1982 (49 U.S.C. § 471, Section 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex)
- 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 Federal-Aid recipients, sub-recipients, and contractors, whether such programs or activities are Federally funded or not)
- Title II and III of the Americans with Disabilities Act (42 U.S.C. §§ 12131-12189), as implemented by Department of Transportation regulations at 49 CFR parts 37 and 38 (prohibits 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)
- The Federal Aviation Administration's Non-Discrimination Statute (49 U.S.C. § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex)
- Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations (ensures non-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)
- Executive Order 13166, Improving Access to Services for People 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)
• Title VIII of the Civil Rights Act of 1968 (Fair Housing Act), as amended (prohibits discrimination in the sale, rental, and financing of dwellings on the basis of race, color, religion, sex, national origin, disability, or familial status (presence of child under the age of 18 and pregnant women)
• Title IX of the Education Amendments Act of 1972, as amended (20 U.S.C. 1681 et seq.) (prohibits discrimination on the basis of sex in education programs or activities)
• Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA 38 U.S.C. 4301-4335) (prohibits discrimination on the basis of present, past or future military service)

47. Communication Prohibitions:

From the issuance date of this procurement until a contract is awarded, there may be no communications concerning the procurement between any vendor and any employee of ODOT in the issuing office, or any other ODOT employee, or any other individual regardless of their employment status, who is in any way involved in the development of the procurement or the selection of the contractor.

The only exceptions to this prohibition are as follows:

1. Communications conducted pursuant to the, Prebid Questions, Discrepancies, and Clarifications Process.

2. As necessary in any pre-existing or on-going business relationship between ODOT and any vendor that could submit a proposal in response to this procurement;

3. As part of any vendor interview process or proposal clarification process initiated by ODOT, which ODOT deems necessary in order to make a final selection;

4. If it becomes necessary to revise any part of this procurement, ODOT will post those revisions, amendments, etc., to the website; and

5. Any Public Records Request (PRR) made through the proper channels.

ODOT is not responsible for the accuracy of any information regarding this procurement that is obtained or gathered through a source other than the Q&A process described in this procurement. Any attempts at prohibited communications by vendors may result in the disqualification of those vendors’ proposals.

If interested vendors have a need to communicate regarding this procurement, they must contact ODOT using one of the mechanisms provided for in the, Prebid Questions, Discrepancies, and Clarifications Process. Vendors are cautioned that communication attempts which do not comply with these instructions will not be answered, and that ODOT will not consider any proposals submitted anywhere other than the delivery method provided in this procurement. Vendor proposals must be submitted to ODOT in strict accordance with proposal submission instructions provided in the procurement document.

(the remainder of this page has been left intentionally blank)
AFFIRMATION AND DISCLOSURE FORM

By the signature affixed hereto, the Contractor affirms and understands that if awarded a contract, both the Contractor and any of its subcontractors shall perform no services requested under this Contract outside of the United States, not allow State data to be sent, taken, accessed, tested, maintained, backed-up, stored or made available remotely(located) outside of the United States unless a duly signed waiver from the State has been attained.

The Contractor shall provide all the name(s) and location(s) where services under this Contract will be performed and where data is located in the spaces provided below or by attachment. Failure to provide this information may result in no award. If the Contractor will not be using subcontractors, indicate “Not Applicable” in the appropriate spaces.

EXPENDITURE OF PUBLIC FUNDS ON SERVICES PERFORMED BY RUSSIAN COMPANIES OR INSTITUTIONS.
The Contractor affirms to have read and understands Executive Order 2022-02D and shall abide by those requirements in the performance of this Contract. Pursuant to this Executive Order, all state agencies are prohibited from the purchase of services from Russian companies or institutions. This prohibition is in addition to and expands upon Executive Order 2019-12D which generally precludes the purchase of offshore services by the State of Ohio. Notwithstanding any other terms of this Contract, ODOT reserves the right to recover any funds paid for services the Contractor performs in Russia in violation of this Executive Order. ODOT does not waive any other rights and remedies provided to ODOT in this Contract.

The Contractor agrees to complete the attached Exhibit II, Contractor/Subcontractor Affirmation and Disclosure Form, to abide with Executive Order 2022-02D, which is incorporated and becomes a part of this Contract, affirming no services of the Contractor or its subcontractors under this Contract will be performed in Russia.

1. Principal location of business of Contractor:

   __________________________________________ (City, State, Zip)
   (Address)      (City, State, Zip)

   Name/Principal location of business of subcontractor(s):

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)

2. Location where services will be performed by Contractor:

   __________________________________________ (City, State, Zip)
   (Address)      (City, State, Zip)

   Name/Location where services will be performed by subcontractor(s):

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)

3. Location where state data will be located, by Contractor:

   __________________________________________ (City, State, Zip)
   (Address)      (City, State, Zip)

   Name/Location(s) where state data will be located by subcontractor(s):

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)

   __________________________________________ (Address, City, State, Zip)
   (Name)      (Address, City, State, Zip)
Invitation No. 524-23

Contractor also affirms, understands and agrees that Contractor and its subcontractors are under a duty to disclose to the State any change or shift in location of services performed by Contractor or its subcontractors before, during and after execution of any contract with the State. Contractor agrees it shall so notify the State immediately of any such change or shift in location of its services. The State has the right to immediately terminate the contract, unless a duly signed waiver from the State has been attained by the Contractor to perform the services outside the United States.

On behalf of the Contractor, I acknowledge that I am duly authorized to execute this Affirmation and Disclosure Form and have read and understand that this form is a part of any Contract that Contractor may enter into with the State and is incorporated therein.

By: __________________________________________
    Contractor

Print Name: _______________________________
Title: ___________________________________
Date: ___________________________________

(the remainder of this page has been left intentionally blank)
## District Map

### Ohio Department of Transportation

#### District Information

<table>
<thead>
<tr>
<th>District</th>
<th>District Deputy Director, District Address</th>
<th>Main Telephone No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1885 N. McCullough, Lima, Ohio 45801</td>
<td>419-222-9055</td>
</tr>
<tr>
<td>2</td>
<td>317 East Poe Road, Bowling Green, Ohio 43402</td>
<td>419-353-8131</td>
</tr>
<tr>
<td>3</td>
<td>906 North Clark St., Ashland, Ohio 44805</td>
<td>419-281-0513</td>
</tr>
<tr>
<td>4</td>
<td>2088 S. Arlingon Rd., Akron, Ohio 44306</td>
<td>330-786-3100</td>
</tr>
<tr>
<td>5</td>
<td>9600 Jackstown Road, P.O. Box 306, Jackstown, Ohio 43030</td>
<td>740-323-4400</td>
</tr>
<tr>
<td>6</td>
<td>400 East Williams St., Delaware, Ohio 43015</td>
<td>740-363-1251</td>
</tr>
<tr>
<td>7</td>
<td>1001 St. Mary’s Ave, Sidney, Ohio 45365</td>
<td>937-492-1141</td>
</tr>
<tr>
<td>8</td>
<td>505 South State Rt. 741, Lebanon, Ohio 45036</td>
<td>513-932-3030</td>
</tr>
<tr>
<td>9</td>
<td>650 Eastern Ave., P.O. Box 467, Chillicothe, Ohio 45601</td>
<td>740-773-2691</td>
</tr>
<tr>
<td>10</td>
<td>338 Muskingum Drive, Marietta, Ohio 45750</td>
<td>740-373-0212</td>
</tr>
<tr>
<td>11</td>
<td>2201 Reiser Ave SE, New Philadelphia, Ohio 44663</td>
<td>330-339-6633</td>
</tr>
<tr>
<td>12</td>
<td>5500 Transportation Boulevard, Garfield Heights, Ohio 44125-5396, Mail: Box 258003, Garfield Heights, Ohio 44125-8003</td>
<td>216-581-2100</td>
</tr>
</tbody>
</table>
State of Ohio, Department of Transportation (ODOT)  
Office of Contract Sales, Purchasing Services  

SIGNATURE PAGE  
Procurement # 524-23  
Commodity/Service: Trip Coordination Scheduling and Dispatching Software  

This Signature Page must be completed and submitted with a Bidder’s sealed bid package to serve as acknowledgement to the Department that the Bidder understands and will comply with all terms, conditions, and requirements in submitting a response for the above-referenced procurement.  

Furthermore, the execution and submission of this Signature Page shall serve as acknowledgment that the Bidder will enter into a Contract with the State of Ohio, Department of Transportation if selected for award of the above-referenced procurement, and understands, upon Contract award, it shall be bound by all terms and conditions included in this procurement.  

The person signing and executing this Signature Page below acknowledges that he/she is signing on behalf of their Company in a representative capacity and hereby warrants that he/she has been duly authorized by his/her Company to submit this formal response and is authorized to execute Contracts on such Company’s behalf.  

(Please execute below)  

Company (Bidder) Name: ________________________________________________________  
Original Signature: _____________________________________________________________  
Print Name of Officer: ___________________________________________________________  
Title of Signing Officer: __________________________________________________________  
Date: _________________________________________  

FOR USE BY THE OHIO DEPARTMENT OF TRANSPORTATION ONLY:  
Pursuant to Section 30 of the Instructions, Terms and Conditions for Bidding, a signature below by the Director of ODOT shall serve as the Department’s formal acceptance of the bidder’s offer and will effectively form ODOT Contract  524-23 between the State of Ohio, Department of Transportation and the above successful bidder (company):  

Nathan Fling, Signing on behalf of Director of Transportation, Jack Marchbanks  

Jack Marchbanks, Ph. D.  
Director  
State of Ohio, Department of Transportation
### Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/01/2019</td>
<td>Original Version</td>
</tr>
<tr>
<td>10/18/2019</td>
<td>Updated to modify service descriptions, include new services, and remove older services. A new Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements was added.</td>
</tr>
<tr>
<td>12/15/2020</td>
<td>Updated to align with current service offerings, to incorporate the Cloud Smart strategy, and to clarify the variance request requirements.</td>
</tr>
<tr>
<td>5/13/2021</td>
<td>Updated to align with current Infrastructure as a Service (IaaS) Frameworks service offering.</td>
</tr>
<tr>
<td>7/19/2021</td>
<td>Updated to modify service descriptions, include new services, and remove older services.</td>
</tr>
<tr>
<td>02/07/2022</td>
<td>Updated Section 4.1. State IT Cloud Smart Strategy to clarify the scope, intent, and requirements of the service. Also, reorganized the public and private cloud information.</td>
</tr>
</tbody>
</table>
Contents

1. Overview of Supplement and Requirements .................................................................................................................. 4
2. Proposed Variances to Supplement Requirements ........................................................................................................ 4
3. State IT Policy and Standard Requirements .................................................................................................................. 4
4. State of Ohio IT Services .................................................................................................................................................... 5
   4.1. State IT Cloud Smart Strategy ......................................................................................................................................... 5
      4.1.1. Public Cloud Brokerage Service ............................................................................................................................. 6
      4.1.1.1. IaaS Cloud Brokerage Service ......................................................... 6
      4.1.1.2. PaaS Cloud Brokerage Service ..................................................... 6
      4.1.1.3. Vendor Managed Cloud Brokerage Service ................................ 7
      4.1.2. Private Cloud Data Center Services ............................................................ 7
      4.1.2.1. AIX Systems .................................................................................. 7
      4.1.2.2. Enterprise Backup Services ......................................................... 7
      4.1.2.3. Data Center Co-Location Service .................................................. 7
      4.1.2.4. Enterprise Data Storage ................................................................ 8
      4.1.2.5. Open Systems DR-DRaaS ............................................................. 8
      4.1.2.6. Mainframe Business Continuity and Disaster Recovery ........... 8
      4.1.2.7. Mainframe Systems ....................................................................... 9
      4.1.2.8. Metro Site Facility ......................................................................... 9
      4.1.2.9. Server Virtualization .................................................................... 9
   4.2. InnovateOhio Platform .................................................................................................................................................. 9
      4.2.1. Digital Identity Products ................................................................... 10
      4.2.2. User Experience Products ............................................................... 10
      4.2.3. Data and Analytics Products ............................................................ 11
   4.3. Enterprise Application Services .................................................................................................................................. 12
      4.3.1. Application Services ......................................................................... 12
      4.3.2. Enterprise Hosted Document Management ...................................... 12
      4.3.3. Electronic Data Interchange (EDI) Application Integration .......... 12
      4.3.4. Enterprise Business Intelligence ...................................................... 13
      4.3.5. eLicense Ohio Professional Licensure .............................................. 13
      4.3.6. ePayment Business Solutions ....................................................... 14
      4.3.7. Enterprise eSignature Service ......................................................... 14
      4.3.8. Identity Management ....................................................................... 14
      4.3.9. IT Service Management Tool (ServiceNow)................................... 14
      4.3.10. Automated Ticketing ..................................................................... 15
      4.3.11. Ohio Benefits ................................................................................ 15
      4.3.12. Ohio Business Gateway (OBG) ..................................................... 16
      4.3.13. Ohio Administrative Knowledge System (OAKS) .................... 16
      4.3.14. Enterprise Geocoding ................................................................. 17
      4.3.15. Geographic Information Systems (GIS) Hosting ....................... 17
   4.4. Hosted Services ............................................................................................................................................................. 17
      4.4.1. Enterprise SharePoint ....................................................................... 17
      4.4.2. Database Support ........................................................................... 18
   4.5. IT Security Services ........................................................................................................................................................ 18
   4.6. Messaging Services ....................................................................................................................................................... 19
4.6.1. Microsoft License Administration (Office 365) .......................................................... 19

4.7. Network Services .............................................................................................................. 19
  4.7.1. Ohio One Network ........................................................................................................ 19
  4.7.2. Secure Authentication .................................................................................................. 19
  4.7.3. Wireless as a Service ................................................................................................... 20

4.8. Telephony Services ........................................................................................................... 20
  4.8.1. Voice Services – VoIP ................................................................................................. 20
  4.8.2. Toll-Free Service ......................................................................................................... 20
  4.8.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers ................................................................. 20
  4.8.4. Call Recording ........................................................................................................... 20
  4.8.5. Conferencing .............................................................................................................. 21
  4.8.6. Fax2Mail ..................................................................................................................... 21
  4.8.7. Session Initiation Protocol (SIP) Call Paths ............................................................... 21
  4.8.8. Site Survivability ........................................................................................................ 21
  4.8.9. VoIP related Professional Services and Training ...................................................... 21

Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements ................................................ 22
1. Overview of Supplement and Requirements

This supplement shall apply to any and all work, services, locations and computing elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State of Ohio (“State”) and any access to State resources in conjunction with delivery of work.

This includes, but is not limited to:

- Major and minor projects, upgrades, updates, fixes, patches and other software and systems inclusive of all State elements or elements under the Contractor’s responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized change orders, change requests, statements of work, extensions or amendments to this contract;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-contracted personnel that have access to State Data as defined below:
  - “State Data” includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.
  - “Sensitive Data” is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. Sensitive Data includes but is not limited to:
    - Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.
    - Federal Tax Information (FTI) under IRS Special Publication 1075.
    - Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).
    - The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in the Contract shall prevail.

Contractors performing the work under the Contract are required to comply with Ohio and the Ohio Department of Administrative Services (DAS) Office of Information Technology (OIT) (“DAS OIT”) policies and standards (refer to Section 3 for additional information) and leverage State IT services outlined in this document unless the State has approved a variance. Refer to Section 2 for instructions on proposing variances to the requirements outlined in this supplement.

2. Proposed Variances to Supplement Requirements

ANY PROPOSED VARIANCES TO THE REQUIREMENTS OUTLINED IN THIS SUPPLEMENT ARE REQUIRED TO BE IDENTIFIED IN APPENDIX A - REQUEST FOR VARIANCE TO STATE IT POLICY, STANDARD OR SERVICE REQUIREMENTS. OFFERORS ARE ASKED NOT TO MAKE ANY CHANGES TO THE LANGUAGE CONTAINED WITHIN THIS SUPPLEMENT. In the event the Offeror finds it necessary to deviate from any of the IT policies, standards or State IT services, a variance may be requested, and the Offeror must provide a sufficient business justification for the variance request. In the event that a variance is requested post award (e.g., a material change to the architecture), the Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

3. State IT Policy and Standard Requirements

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in the table below.
Table 1 – State of Ohio IT Policies, Standards, IT Bulletins and DAS Policies

<table>
<thead>
<tr>
<th>Item</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAS Policies</td>
<td>100-11 Protecting Privacy</td>
</tr>
<tr>
<td></td>
<td>100-12 ID Badges &amp; Visitors Policy</td>
</tr>
<tr>
<td></td>
<td>700-00 – Technology / Computer Usage Series</td>
</tr>
<tr>
<td></td>
<td>2000-00 – IT Operations and Management Series</td>
</tr>
<tr>
<td></td>
<td><a href="https://das.ohio.gov/Divisions/Administrative-Support/">https://das.ohio.gov/Divisions/Administrative-Support/</a> Employees-Services/DAS-Policies</td>
</tr>
</tbody>
</table>

Please affirm compliance with the State’s IT policies and standards. If this section, or portions of this section are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4. State of Ohio IT Services

DAS OIT delivers information technology (IT) and telecommunication services. DAS OIT is responsible for operating and maintaining IT and telecommunication hardware devices, as well as the related software. The supplement outlines a range of service offerings from DAS OIT that enhance performance capacity and improve operational efficiency. Explanations of each service are provided and are grouped according to the following solution categories. Where applicable, Contractors are required and expected to incorporate these services into their solutions or provided services.

4.1. State IT Cloud Smart Strategy

Executive Order 2019-15D, “Modernizing Information Technology Systems in State Agencies,” required all cabinet agencies, boards and commissions to migrate information technology systems to the State’s cloud environment managed by DAS OIT. From this executive order, the State IT Cloud Smart Strategy (“Strategy”) evolved to support agency cloud service needs. The Strategy is designed to provide a value-driven, dynamic, and cost-effective set of differentiating core enterprise services and innovative technologies from public and private clouds that will improve State of Ohio operations and the quality of services to Ohioans.

As part of the Strategy, DAS OIT will operate a Cloud Center of Excellence (“CCoE”) to focus on leveraging the State’s investment in the private cloud, while incorporating efficiencies from public cloud providers. The CCoE provides guidance that will assist in realizing the value of a multi-cloud investment. The goal is to evaluate and provide the most optimal hosting environment in the State’s public and/or private clouds. The CCoE offers an Enterprise Cloud Brokerage Service (“Brokerage Service”) that supports and guides State Agencies (“Agencies”) as they look to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) application and solution modernization opportunities.

The Strategy requires any proposed customized applications running on an IaaS or PaaS public cloud to reside in the Brokerage Service (Microsoft Azure, Amazon Web Services, Oracle Cloud Infrastructure, Google Cloud Platform or IBM Cloud). Applications developed and hosted in low code or no code platforms (e.g., Salesforce, Power Apps, or ServiceNow) will not reside within the Brokerage Service and will be addressed on a case-by-case basis.

Any proposed statewide or individual Agency solution must comply with the Strategy.

1 Customized Applications: In terms of this Supplement, this term refers to applications that are specifically written, modified, or adapted for the State of Ohio.
4.1.1. Public Cloud Brokerage Service

DAS OIT is leading the effort to transform how IT services are delivered, maintained, and consumed in the State of Ohio. A key outcome of this digital transformation is the development of cloud-based capabilities that will improve the quality of services, agility, and foster a culture of collaboration, accountability, and innovation.

This service is available on multiple public clouds: Microsoft Azure, Amazon Web Services, Oracle Cloud Infrastructure, Google Cloud Platform and IBM Cloud.

Within the Public Cloud Brokerage Service model, DAS OIT offers IaaS, PaaS, and vendor managed frameworks. These service offerings are described in detail in the sections below.

4.1.1.1. IaaS Cloud Brokerage Service

The IaaS Cloud Brokerage Service is a DAS OIT managed service similar to the Private Cloud Data Center. DAS OIT will architect, configure and run all IaaS implementations, whether on premises or in a public cloud. The same tools are used to update, secure, and manage the virtual machines, no matter the location (private or public cloud).

Within the established framework for each public cloud, the customer has read access to their infrastructure running in a specific public cloud. The customer cannot create or manage compute items without receiving an approved exemption due to Executive Order 2019-15D referenced above. While customers cannot create any network peering, they can request peering back to the State Private Cloud via dedicated private connections.

IaaS Cloud Brokerage Service offers:
- Configuring network security groups and backups
- Performing restores
- Storage
- Providing a direct network connection to the State of Ohio Computer Center from public cloud vendor locations
- Managing and monitoring using the same tools as the Private Cloud
- Patching
- Design consultation
- Education
- Offering specific cloud expertise, when needed

4.1.1.2. PaaS Cloud Brokerage Service

The PaaS Cloud Brokerage Service offers customers the ability to request an environment in one of the State’s public clouds. The PaaS environment allows the customer to consume the appropriate cloud native services.

Within the established framework for each public cloud, the customer can create and manage available PaaS cloud offerings.

PaaS Cloud Brokerage Service offers:
- Vendor management
- Providing the initial framework for build and configuration
- Service provisioning, implementation, monitoring and alerting
- Role-Based Access Control Security
- Enforcing Base Compliance Policies
- Active directory account integration, when appropriate
- Assistance in service request resolution via the native cloud portal and the DAS OIT Customer Service Center
- Design consultation

(Please Note: If the Offeror feels that these requirements cannot be accommodated, an explanation must be provided at the end of this section and a proposed variance needs to be defined in Appendix A.)
• Education
• Offering specific cloud expertise, when needed

4.1.1.3. Vendor Managed Cloud Brokerage Service

The Vendor Managed Cloud Brokerage Service is a vendor-managed application infrastructure within the State’s public cloud framework pursuant to a contract entered into between a customer and the managing vendor.

Operating within this environment helps to ensure that the State’s data remains in the U.S., the initial build and configuration is within the State’s framework and overlap is avoided in the IP (Internet Protocol) space through network addressing standards.

In terms of the Vendor Managed Cloud Brokerage Service, the Brokerage Service is responsible for:

• Vendor management
• Providing the initial framework for build and configuration
• Role-Based Access Control Security
• Design consultation
• Education
• Offering specific cloud expertise, when needed

If the proposed solution cannot accommodate the State’s Strategy and CCoE requirements listed above, please provide a justification for the exception in the space below. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the Supplement shall not be modified.

4.1.2. Private Cloud Data Center Services

4.1.2.1. AIX Systems

Advanced Interactive Executive (AIX) is a proprietary version of the UNIX operating system developed by IBM. The AIX Systems Service enables customers to develop and run applications and/or databases without incurring the cost of setting up, administering and maintaining an operating system environment. DAS OIT runs the AIX operating system on IBM Power hardware, as a physical server or logical partition (LPAR)/virtual server. All of the AIX systems are connected to the DAS OIT Enterprise Storage Area Network (SAN) for performance, general purpose or capacity based storage. All systems are also provided backup and recovery services.

4.1.2.2. Enterprise Backup Services

The Enterprise Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of customer data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available for customer data. DAS OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

4.1.2.3. Data Center Co-Location Service

The DAS OIT Co-Location service offers customers a Tier 3 capable secure data center environment with reliable uptime, power redundancy and redundant cooling to ensure uninterrupted access of critical data and applications in the State of Ohio Computer Center (SOCC). The SOCC is staffed and available to authorized personnel 24 x 7 x 365 and is accessible via electronic card key only.
4.1.2.4. Enterprise Data Storage

DAS OIT will work with the Contractor and customer to determine the optimal data storage solution, if applicable. The services covered under Enterprise Data Storage include:

- **High Performance Disk Storage** service offers high-performance, high-capacity, secure storage designed to deliver the highest levels of performance, flexibility, scalability and resiliency. The service has fully redundant storage subsystems, with greater than five-nines availability, supporting mission critical, customer-facing and revenue-generating applications 24x7x365. High Performance Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

- **General Purpose Disk Storage** service offers a lower-cost storage subsystem for customers not requiring high performance disk. This service supports a wide range of applications, including email, databases and file systems. General Purpose Disk is also flexible and scalable and highly available. General Purpose Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

- **Capacity Disk Storage** service is the least expensive level of disk storage available from DAS OIT. Capacity Disk is suitable for large capacity, low performance data, such as test, development and archival. Capacity Disk Storage is supplied as dual Enterprise SAN fiber attached block storage or as file based storage.

4.1.2.5. Open Systems DR-DRaaS

Open Systems Disaster Recovery as a Service (DRaaS) offers server imaging and storage at a geographically disparate site from Columbus, Ohio. The service provides customers with a private Disaster Recovery as a Service solution connected to the SOCC via the Ohio One Network that will consists of the following:

- Compute to allow expected performance in the event of a complete failover
- 24vCPU per host with 32 host in the environment all licensed with VMware
- Support of the orchestration and replication environment
- Site connectivity
- Stored images available upon demand

**Open Systems Disaster Recovery - Windows (1330 / 100607 / DAS505170/ 3854L)** - Open Systems Disaster Recovery – Windows is a service that provides a secondary failover site for Windows based servers within the geographically disparate site. This service provides duplicative server compute and storage to match Server Virtualization and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

**Open Systems Disaster Recovery - AIX (1330 / 100607 / DAS505170/ 3854N)** - Open Systems Disaster Recovery – AIX is a service that provides a secondary failover site for AIX based servers within the geographically disparate site. This service provides duplicative server compute and storage to match AIX Systems Services and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

4.1.2.6. Mainframe Business Continuity and Disaster Recovery

Business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery, a subset of business continuity focuses on restoring the information technology systems that support the business functions.

Mainframe Disaster Recovery (DR) services are offered to customers of DAS OIT’s IBM mainframe environment. Services are made available via IBM’s Business Continuity and Resiliency Services which provides hot site computer facilities at a remote location.

Tests are conducted annually at IBM’s hot site location, during which DAS OIT’s mainframe computer infrastructure is restored. Once the mainframe system is operational, participating Agencies restore their production applications and conduct extensive tests to ensure that those applications have been successfully recovered and would be available in the event of an actual disaster.
This service is designed to expand business continuity and disaster recovery capabilities in the most cost effective and efficient manner possible for DAS customers and for Agencies that have systems and applications that run on DAS/OIT infrastructure at the SOCC.

4.1.2.7. Mainframe Systems

DAS OIT’s Mainframe Systems services offer an IBM mainframe computer sysplex with a processing speed rating at 5052 Million of Instructions per Second (MIPS). This mainframe uses the z/OS operating system and the Job Entry Subsystem (JES3). Additionally, the system is connected via fiber to DAS OIT’s High Performance Disk Storage, which affords reliable and fast disk access and additional storage capacity when needed.

Services are provided using a wide range of application, transaction processing and telecommunications software. Data security and user authentication are provided by security software packages. This service enables customers to develop applications without incurring the costs of setting up and maintaining a mainframe operating system environment.

Mainframe tape service option is available:

- Mainframe Virtual Tape - Virtual tape technology that optimizes batch processing and allows for better tape utilization using the EMC Disk Library for Mainframe (DLM) virtual tape.

4.1.2.8. Metro Site Facility

The Metro Site Facility Service provides a secondary, near real-time (measured in milliseconds) failover from the SOCC. This service provides for the facility, site connectivity, on-going support of server images for Disaster Recovery as a Service, and associated services. Metro Site Facilities are offered to support Virtual Server and Data Storage customers providing Global/Metro Mirroring at a secondary near real time failover site within the Metro Columbus area. This service provides duplicative server facilities to match Server Virtualization and Data Storage Rates. Storage necessary for support of the disaster recovery image will be billable at the standard storage rates.

4.1.2.9. Server Virtualization

Server Virtualization is the practice of abstracting the physical hardware resources of compute, storage and networking of a host server and presenting those resources individually to multiple guest virtual servers contained in separate virtual environments. DAS OIT leverages the VMware vSphere platform to transform standardized hardware into this shared resource model that is capable of providing solutions around availability, security and automation.

Server Virtualization includes:

- **OIT Managed-Basic Server Virtualization**: DAS OIT hosts the virtual server and manages the hardware/virtualization layer. DAS OIT is also responsible for managing the server’s operating system (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of General Disk Storage used for the operating system.

If the proposed solution cannot accommodate the State’s Private Cloud Data Center Services listed above, please provide a justification for the exception in the space below. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.2. InnovateOhio Platform
Executive Order 2019-15D, “Modernizing Information Technology Systems in State Agencies,” established the InnovateOhio Platform (IOP) initiative. IOP focuses on digital identity, the experience of the individual authorized to access the system (“User”), analytics and data sharing capabilities. The InnovateOhio Platform provides integrated and scalable capabilities that better serve Ohioans.

4.2.1. **Digital Identity Products**

**OH | ID - Digital identity solution for Ohio citizens:**
Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for citizens. Multiple levels of identity assurance.

- Single Sign-On
- Access Logging
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Access Management
- Self-Service Portal
- Identity Proofing
- Directory Integration

**OH | ID Workforce - Digital identity solution for Ohio workforce**
Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for state and county employees, contractors, and external workers. Multiple levels of identity assurance.

- Single Sign-On
- Directory Integration
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Just-in-Time Provisioning
- User Management
- Access Logging
- Privileged Access Management

**ID Platform – Software as a Service (SaaS) identity framework**
Provides authorization layer for use by Agencies and programs. Allows Agencies to integrate and extend InnovateOhio Platform identity services into their applications. Customizable to Agency needs.

- Fine-Grain Authorization Management
- Real-Time Analytics
- Extendable Services from OH|ID
- Cloud-Based Infrastructure

4.2.2. **User Experience Products**

**IOP Portal Builder - Website template accelerator:**
An accelerator to easily create modern, responsive, and ADA-compliant websites and portals for the InnovateOhio cloud platform. The InnovateOhio Portal Builder is available in a Software as a Service (SaaS) form.

- Standardized Dynamic Templates
- Automated Workflows
- Governance & Access Control
- Optimized Content Search
- ADA-Compliant
- Content Management
- Integration with OH|ID
- Real-Time Analytics
- Aggregate Applications
- Customizable Features
- Mobile Ready
- Site Analytics

**IOP myOhio - The State’s Intranet platform**
Features intuitive navigation, simplified access to on-boarded business applications, and a modernized, mobile-responsive design. Automates compliance with accessibility standards per Section 508 of the Rehabilitation Act.

- Single Sign-On
- Personalized Content
- Content Management
- Near Real-Time Syndication
- 2-Factor Authentication (2FA)
- Access Logging
- Optimized Content Search
- Application Store
- Automated Workflows
- Real-Time Analytics
- Site Analytics
IOP Digital Toolkit - Free User experience digital toolkit
Reusable components for quick deployment of websites, portals and applications. Universal framework for developers and designers. Consistent and compliant User experiences.

- Mobile Ready
- Real-Time Analytics
- Style Guide
- Customizable Features

- Sample Code
- ADA-Compliant
- Standardized Dynamic Templates

4.2.3. Data and Analytics Products

IOP Applied Analytics
Provides the ability to build analytical and reporting solutions and deploy them in the most impactful manner possible by putting data in the hands of Users in their natural workflow. The applied analytics solution enables User to move from concept to results.

- BI Reporting
- Query Exploration
- Data Science

- Visual Analytics
- Embedded Analytics

IOP Data Integration
Provides the capability to combine information from a wide array of sources, applications and formats so that it can be analyzed to derive valuable business insights. Furthermore, data ingestion pipelines can be automated and governed, while ensuring secured access to the data.

- Data Gateways
- Workload Automation

- Data Ingestion
- Real-time Streaming

IOP Data Management
Provides rich and secure capabilities to harness the power of the analytics platform leveraging user friendly and pre-configured technologies. Additionally, the product supports a bring-your-own-tool approach allowing analysts and data scientists to work on the platform with the technologies they are most comfortable using.

- Audit
- Data Catalog
- Data Prep and Profile
- Data Warehousing
- Relational Search
- Bring Your Own Tool
- Data Lineage

- Data Sharing
- De-identification
- Code Management
- Data Portability
- Data Transformation
- Entity Resolution

IOP Service Offerings
Services, support, and training to successfully engage and onboard agencies to perform applied analytics work on the Platform.

- DataOhio Portal
- Data Onboarding
- Development Services
- Engagement

- Project Support
- Solution Design & Architecture
- Training Resources
- Use Case Development

Please explain how the InnovateOhio Platform will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.
4.3. Enterprise Application Services

4.3.1. Application Services

Application Services provides standardized, integrated solutions for Application Development. The core components of the solution include:

- **Application Development Lifecycle Services** for creating new applications and systems.
- **Application Development Operations** for maintaining and enhancing existing applications and systems.
- **Website Lifecycle Services** for designing and creating new websites.
- **Website Operations** for maintaining and updating existing websites.
- **User Interface/User Experience Services** that work in connection with Application Development and Website work that define the "look and feel" of what users interact with.

**Supporting Technology Services** which support the Applications, Systems and Websites developed. These services can include payment processing, application performance monitoring, and complex reporting/visualizations.

4.3.2. Enterprise Hosted Document Management

The Enterprise Hosted Document Management is a standardized, integrated solution for document and content management. The core components of the solution include:

- **Document Management** core capabilities such as: secure check-in / check-out, version control, and index services for business documents, audio / video files, and Environmental Systems Research Institute (ESRI) / Geographic Information Systems (GIS) maps.
- **Image Processing** for capturing, transforming and managing images of paper documents via scanning and / or intelligent character recognition technologies such as Optical Character Recognition.
- **Workflow / Business Process Management (BPM)** for supporting business processes, routing content, assigning work tasks and creating audit trails.
- **Records Management** for long-term retention of content through automation and policy, ensuring legal, regulatory and industry compliance.
- **Web Content Management (WCM)** for controlling content including content creation functions, such as templating, workflow and change management and content deployment functions that deliver content to Web servers.
- **Extended Components** can include one or more of the following: Digital Asset Management (DAM), Document Composition, eForms, search, content and analytics, email, and information archiving.

4.3.3. Electronic Data Interchange (EDI) Application Integration

The EDI Application Integration service is a combination of Application Integration, Data Exchange and Electronic Data Interchange (EDI) functionality. This service provides application to application connectivity to support interoperable communication, data transformation, and business process orchestration amongst applications on the same or different computing platforms. Business process orchestration between many data formats may be supported including Web Services, XML, People-Soft, FTP, HTTP, MSMQ, SQL, Oracle, Flat File, SAP, DB2, CICS, EDI, HIPAA, HL7, Rosetta Net, etc.

The Data Exchange component allows unattended delivery of any electronic data format to a customer via encrypted files over public FTP, FTPS, SFTP, VPN.

Application Integration services are offered via:

- **End Points** – also referred to as a mailbox, this is a connectivity point to facilitate the movement or transaction of data between two or more entities.
- **KBs** – represents the size in kilobytes of a message that is transformed or processed. This typically refers to a document or file conversion or a format change.
- **Messages** – a discrete unit of data that is moved or transacted between two or more entities. A message typically represents a business document or a file.
4.3.4. Enterprise Business Intelligence

The State of Ohio Enterprise Business Intelligence (BI) service provides reporting, data visualization, enterprise data warehousing, business and predictive analytics, and decision support solutions to Users from all 120+ state agencies, boards and commissions, and institutions of higher education. With tools such as Cognos and Tableau, the Enterprise BI team can help turn raw data into usable information and powerful visualizations, in turn helping Users analyze policies and programs, evaluate operations and drive decisions.

Enterprise BI Solutions — Standardized reporting solutions to benefit all Agencies.

- **Financial Information Cost and Spend Management** – Agencies can gain valuable insights into planned, actual, and forecasted spending based on historical information as well as planned expenditures, budgets, and actual results.
- **Workforce and Human Resources** – Agencies can gain valuable insights into position management, workforce composition, pay, leave and benefits, and more.
- **Targeted Solutions** – The BI Team currently provides data visualization solutions to Agencies and custom reporting solutions to 50+ Agencies, with availability for additional options ranging from consultations through turn-key content delivery.

BI Core Reporting Services include:

**Financial Information**
- Enterprise Financial Dashboards
- General Ledger
- Budget and Planning (BPM)
- Travel and Expense
- Procure to Pay
- Accounts Receivable
- Asset Management
- Value Management
- Trends and Forecasts
- Statewide Cost Allocation Plan (SWCAP)
- MBE/EDGE and Equal Opportunity
- State of Ohio Payroll Projection Systems (SOPPS)

**Workforce and Human Resources**
- Enterprise HR Dashboards
- Workforce Profile
- Compensation
- ePerformance/ePAR
- Enterprise Learning Management

**50+ Targeted Solutions including:**
- Interactive Budget OBM
- Higher Education OHDE
- JFS dashboards
- State Health Facts
- BWC Core Reporting

4.3.5. eLicense Ohio Professional Licensure

eLicense Ohio Professional Licensure is the State of Ohio’s online system used to manage the issuance, certifications, inspections, renewals and administration of professional licenses across the State. The eLicense application is a public/business facing system that is designed to foster the creation and growth of businesses in the State and is the mechanism through which state agencies, boards and commissions support Ohioans. The system is a central repository for license and certificate data, in addition to managing the generation and storage of correspondence. Secure fee collection is performed through an on-line payment processor, which includes bank transfers, credit cards, and other payment types.

Core system capabilities include:

**Customer Relationship Manager (CRM)**
- Contact Management

**Revenue**
- Deposit Accounting Revenue Tracking
- Refund and Reimbursement Processing
- Fine and Penalty Tracking

**License Administration**
- Administration
- Workflow

**Online Licensure Services**
- Applications
- Renewals
- License Verification
- License Maintenance
- License Lookup Website
- Workflow
- Document Management
- Secure Payment Processing

**Other Services**
4.3.6. ePayment Business Solutions

DAS OIT’s ePayment Business Solution allows State agencies as well as boards and commissions to accept electronic credit card and Automated Clearing House (ACH) payments from customers. The ePayment solution is a highly flexible payment engine supporting a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, remote capture and cash payments.

The solution utilizes a single, common gateway to permit the acceptance of payments from multiple client application sources: Web, IVR, kiosk, POS, mobile, over the counter, etc. Payment processing is supported through multiple credit card gateway options, automated clearing house (ACH) bank processing, and check acceptance services.

The ePayment solution is compliant with the Payment Card Industry Data Security Standard (PCI DSS), the Electronic Fund Transfer Act (EFTA) and is audited to the standards of SSAE16 SOC1 Type II.

4.3.7. Enterprise eSignature Service

OneSpan Sign is Ohio’s enterprise solution for eSignatures. The product is a FedRAMP SaaS (Software as a Service) solution, which offers a standardized approach to cloud security. OneSpan Sign’s eSignature functions include workflows, tracking, audit logs and protection against forgery/non-repudiation.

OneSpan Sign has an extensive library of open application programming interfaces (APIs) to integrate eSignatures with existing applications and core systems. OneSpan Sign’s pre-built, third-party connectors enable the eSignature capabilities into business software products such as Dynamics CRM, Salesforce, Microsoft SharePoint, etc.

4.3.8. Identity Management

Identity Management provides integrated authentication services across multiple enterprise service offerings. The service also streamlines the life cycle events for user credentials including onboarding, provisioning, administration, service consumption, change events, de-provisioning and off-boarding.

Identity Management is made up of four service functions:

- **Identity Repository** offers a centralized container for all user credentials and management tools for the administration of those credentials and credential attributes.
- **Core Shared Services** leverage the centralized credential from the identity repository for authentication. Service provisioning tools are available to provision access to various portions of the core shared services within the Identity Management service.
- **Application Integration** permits an Agency’s line of business application to authenticate to the centralized user credential within the Identity Repository using a secure Lightweight Directory Access Protocol (LDAP) and/or Active Directory Federation (SAML 2.0)
- **Endpoint Consumption** allows for the placement of desktops, laptops, and/or tablets to reside within the Identity Management service. This extends the ability to use a single credential to authenticate to workstations and applications.

4.3.9. IT Service Management Tool (ServiceNow)

DAS OIT offers ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk work-flow based application which provides flexibility and ease-of-use. The IT Service Management Tool provides workflows aligning with Information Technology Infrastructure Library (ITIL) processes such as incident management, request fulfillment, problem management, change management.
and service catalog. These processes allow customers to manage related fields, approvals, escalations, notifications, and reporting needs. Customers have the option of provisioning the entire suite of service features or selecting those features best suited for their needs.

The following modules are currently in use on the enterprise platform:

- IT Service Management
- IT Operations Management
- IT Business Management
- Governance, Risk & Compliance
- Security Operations
- Intelligent Applications

**ServiceNow Product Catalog**

The Product Catalog contains:

- The applications currently in use of the State of Ohio ServiceNow Application across Agencies
- The product wheel of the platform footprint
- Applications in use by Agencies
- Product descriptions by Platform family, then Application within Family for current functionality
- Product descriptions by Platform family, then Application within the Family for services not deployed

### 4.3.10. Automated Ticketing

DAS OIT offers Watson Automated Ticketing that integrates with ServiceNow for Agencies interested in having incidents and requests in their UNASSIGNED queue that comes through email assigned to the proper resolver queue. This service will route these incidents to the appropriated queue based on historical data and optionally provide other use cases as well. Watson is a cognitive automation platform that leverages machine learning, natural language processing, deep learning, semantic ontologies, pattern recognition, etc.

Watson is used for automating manual parts of the support processes using Artificial Intelligence algorithms. It automates processes to provide more efficient operation with higher quality results compared to manual performance.

### 4.3.11. Ohio Benefits

Ohio Benefits provides a comprehensive and effective platform for planning, designing, development, deployment, hosting and ongoing maintenance of all State of Ohio Health and Human Services (HHS) Public Assistance Services and Programs.

Ohio Benefits provides superior eligibility services including citizen self-service, efficient workflow management and coordination, an agile and easily manageable rules engine, improved data quality and decision support capabilities. Ohio Benefits supports improvement in state and county productivity, capability and accessibility of benefits to Ohioans through a robust enterprise system.

The Ohio Benefits platform provides four distinct technology domains:

- **Common Enterprise Portal** – User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability
- **Enterprise Information Exchange** – Discovery Services (Application and Data Integration, Master Data Management (MDM) Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management
- **Analytics and Business Intelligence** – Integration and delivery of analytics through alerts, notifications & reports.
- **Integrated Eligibility** – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs.
Privacy and security are the foundational blocks of the platform which is compliant with all State and federal standards.

### 4.3.12. Ohio Business Gateway (OBG)

The Ohio Business Gateway (OBG) offers Ohio's businesses a time and money saving online filing and payment system that simplifies business' relationships with government Agencies.

Ohio businesses can use OBG to access various services and electronically submit transactions and payments with many Agencies. OBG Electronic Filing also partners with local governments to enable businesses to file and pay selected Ohio municipal income taxes.

OBG Electronic Filing routes data and payment information directly to program administrators at the Agencies so that they may continue to manage the overall account relationship.

Businesses must be registered with an Agency before using OBG Electronic Filing. Selected Agency registrations are available through OBG Electronic Filing. Information about other registrations may be obtained by visiting the ‘Starting a Business’ section of the Ohio Business Gateway (http://business.ohio.gov/). If a registration is not offered on OBG Electronic Filing, the administering Agency will provide information on how to obtain the registration necessary to begin using OBG Electronic Filing services. For Municipal Income Tax Electronic Filing, businesses must first register directly with municipalities before using OBG.

### 4.3.13. Ohio Administrative Knowledge System (OAKS)

The Ohio Administrative Knowledge System (OAKS) is the State’s Enterprise Resource Planning (ERP) system which provides central administrative business services such as Financial Management, Human Capital Management, Content Management, Talent Management, Enterprise Learning Management and Customer Relationship Management.

Core system capabilities include:

**Content Management (myohio.gov)**
- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids and news
- Statewide News
- Password Reset for Active Directory

**Customer Relationship Management (CRM)**
- Contact / Call Center Management

**Enterprise Business Intelligence**
- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven reporting
- Targeted Business Intelligence
- Tableau Analytics and Visualization

**Ohio Learn**
- Training Curriculum Development
- Training Content Delivery
- Training Status Tracking and Reporting
- **NEW:** Ability to extend Training Content to External Learners

**Ohio Recruit**
- 24x7 Recruiting, Reporting and Analytics
- Applicant Tracking and Compliance

**Financial Management (FIN)**
- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eSourcing
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement
- Travel & Expense

**Human Capital Management (HCM)**
- Benefits Administration
- eBenefits
- ePerformance
- Kronos
- Payroll
- Position Management
- Time and Labor
- Workforce Administration
4.3.14. Enterprise Geocoding

OAKS Enterprise Geocoding is the process of determining associated geographic coordinates from other geographic data, such as street addresses or zip codes. With these geographic coordinates, the features can be displayed and analyzed in a Geographic Information Systems (GIS), or the coordinates can be embedded into media such as digital photographs via geotagging.

OAKS Enterprise Geocoding combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for on-line applications or large numbers of addresses can be processed in batch mode. The quality of each address is improved by standardizing it to meet stringent U.S. Postal Service standards.

Leveraging address location information developed and maintained by local government, the OAKS Enterprise Geocoding uses a multi-tiered geocoding process incorporating data from multiple entities to provide Agencies with the most accurate location information available.

4.3.15. Geographic Information Systems (GIS) Hosting

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. Customers can integrate enterprise-level Geographic Information Systems (GIS) with map capabilities and spatial content into new or existing websites and applications. GIS enhances decision support, integrating data from a variety of sources to be analyzed spatially with the results presented in the form of a map.

DAS OIT offers three types of hosted GIS services:

- **Geodata Hosting** provides a platform for customers to deliver online spatial data and content to end users or applications. Online spatial data can be consumed by desktop GIS applications and web-based applications.

- **Geoprocessing** provides access to server-side geoprocessing tools that allow users to publish analytical models for use within desktop applications by remote users or embedded within Internet mapping applications.

- **GIS Map Application** Hosting provides a platform for customers to deliver web-based mapping content to end users.

GIS Hosting can be combined with the Enterprise Geocoding to create a comprehensive web application to locate and display events, customers, or Agency assets on a map in a browser.

Please explain how the State’s Enterprise Application Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.4. Hosted Services

4.4.1. Enterprise SharePoint

The Enterprise SharePoint Service supports both an on premises and cloud environment. Enterprise SharePoint service provides Site Administration, Technical Services/Support for SharePoint and third-party tools (e.g., Nintex) as well as Strategy, Adoption, Operations and Strategic Management within both the Tenant and Farm level for SharePoint related services. Key Services Included: Site Administration and Technical Services:
Basic Services include:
- Site Collection Creation
- How to's from Site Collection Admin/users
- Research Apps and make available to Tenant/Farm
- Consult on SharePoint Online and On Premises needs with Agencies
- Review & Approve 3rd party tool integration
- Incident/Problem Resolution
- Work to eradicate issues in SharePoint Online
- Routine maintenance
- Site to Site Migrations

Additional Services Available:
- Customized Search
- Site Branding & Design
- Migrating content from one environment to SharePoint (e.g., FileShare to OneDrive or SharePoint)
- Rights Management & Data Protection
- Retention Management
- Azure integration
- Customized Applications and Workflows
- Content types, managed metadata, site structure and navigation

Strategy, Operations and Management – Key Services include:
- Program Management
- SOW and contract creation and processing
- Contract Management
- Adoption Service Template & Education
- Lunch ‘n Learns
- Yearly Reporting
- Community Center Intranet Site Management

Services performed for On Premises environment only:
- Configuration Management
- Code Management
- Patching and Software updates
- Farm Backup and Restore
- Refreshing Content Across Development and Staging environments
- Physical Architecture Changes

4.4.2. Database Support

Database Support provides technical assistance for database implementation and usage. Services utilized by customers may include any or all of the following service offerings: installation, upgrade and management of database software, database administration tools and packaged application database products, backup/recovery procedure implementation, monitoring, tuning and troubleshooting.

Please explain how the State's Hosted Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.5. IT Security Services


Secure Sockets Layer (SSL) Digital Certificate Provisioning service provides Secure Sockets Layer Certificate service across multiple enterprise service offerings. SSL certificates are used to provide communication security to various web sites and communications protocols over the internet (ex. Web Servers, Network Devices, Application Servers, Internet Information Server (IIS), Apache, F5 devices and Exchange servers). SSL Digital Certificate Provisioning supports the delegation of administration and reporting processes for each designated customer Agency while leveraging a common portal.

In addition, please review the Security Supplement (Supplement S - State Information Security and Privacy Requirements and State Data Handling Requirements).
Please explain how the State's IT Security Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.6. Messaging Services

4.6.1. Microsoft License Administration (Office 365)

The Office 365 service provides customers the ability to use email, Office 365 ProPlus, instant messaging, online meetings and web conferencing, and file storage all from the Cloud, allowing the customer to access services virtually anytime and from anywhere and includes email archiving and eDiscovery services.

The Office 365 service provides licensing and support for email, Office 365 ProPlus (Outlook, Word, Excel, PowerPoint, Publisher, Teams and OneNote), SharePoint, and OneDrive for Business. Please note that the Office Suite may require agency deployment or agency/end user installation as well as patch management and distribution.

- Email in the Microsoft Cloud
- Office 365 ProPlus
- Teams
- SharePoint Online
- OneDrive for Business

Please explain how the State's Messaging Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.7. Network Services

Offeror’s solutions must work within the State’s LAN / WAN infrastructure.

4.7.1. Ohio One Network

The State of Ohio’s One Network is a unified solution that brings together design, engineering, operations, service delivery, security, mobility, management, and network infrastructure to target and solve key government challenges by focusing on processes, procedures, consistency, and accountability across all aspects of state, city and local government.

Ohio One Network can deliver an enterprise network access experience for their customers regardless of location or device and deliver a consistent, reliable network access method.

4.7.2. Secure Authentication

The DAS OIT Secure Authentication service provides a managed two-factor user authentication solution to protect an Agency’s resource. The authentication function requires the user to identify themselves with two unique factors,
something they know and something they have, before they are granted access. Whether local or remote, this service ensures that only authorized individuals are permitted access to a customer’s environment.

4.7.3. Wireless as a Service

Wireless as a Service is the IT Enterprise Wireless hosted network which allows customers to connect laptops and devices to their data via a wireless interface. This service is an all-inclusive enterprise level wireless LAN solution that offers guest, employee, voice and location-based services with 24/7 target availability.

Coverage is three tiered:
- Broad coverage – small number of Users with low throughput, i.e., public hot spot, warehouse.
- General data use – most common, general computing with robust data performance.
- High-capacity use (Voice) – maximum capacity, high bandwidth Users, i.e., location and tracking service.

Please explain how the State’s Network Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.8. Telephony Services

4.8.1. Voice Services – VoIP

The State of Ohio hosted cloud VoIP service, also known as NGTS (Next Generation Telephony Service) provides core telephony, voice mail, e911, collaboration, video, audio, conferencing, and auto attendant functions. Optional services include automatic call distributor (ACD), interactive voice response (IVR), multi-channel contact center solutions and session initiation protocol (SIP) trunking among a variety of other features. The service was the first business class phone system to offer closed captioning for the hearing impaired, and also includes features for those with vision and mobility impairments.

The following voice services are offered in addition to the State’s hosted VoIP service.

4.8.2. Toll-Free Service

This service provides the capability to incur telephone charges for incoming calls to an 8xx number.

4.8.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers

The Contact Center Enterprise allows callers to fill in CRM forms with information prior to an Agent responding. With IVR and Advanced Data Collection, callers will spend less time in Call Queues. However, during high demand times, callers can be put on Virtual Hold allowing callers to receive a call back when Agents become available. Call recording with screen capture allows the User to monitor, record, store, and QA calls, helping insure a consistent service experience.

This service also includes multi-channel communications including chat, text, SMS and email to afford those trying to contact the State the ability to contact the State in a variety of ways.

4.8.4. Call Recording
This service is available for new VoIP profiles or modifying existing profiles.

4.8.5. Conferencing

This service offers a conferencing service via telephone lines and or TCP/IP networks. It provides voice & video conferencing capabilities within the network and participants can also join in from outside the network.

4.8.6. Fax2Mail

The Fax2Mail is a "hosted" fax solution that allows organizations to seamlessly integrate inbound and outbound fax with their existing desktop email and back-office environments. The Fax2Mail is completely "cloud-based" (SaaS), providing an easy to implement, easy to manage solution requiring no expenditures on hardware or software. The Fax2Mail solves all faxing requirements, including inbound and out-bound fax, both at the computer desktop and from/to back-office systems, ERP applications, and electronic workflows.

4.8.7. Session Initiation Protocol (SIP) Call Paths

The Session Initiation Protocol Call Paths is used to allocate bandwidth. SIP Call paths:

- Provide existing telephony infrastructure with NGTS services.
- Extends infrastructure into the NGTS cloud.
- Leverages existing investment.
- Bridges the gap.
- All of the United States are Local Calls.
- Share video and collaboration.
- Leverage Toll Free offering.
- Centralized trunk savings.

4.8.8. Site Survivability

This service provides reliable communications via multi-feature redundancy for centralized call processing.

4.8.9. VoIP related Professional Services and Training

Training services can be requested for VoIP telephone Users. Professional services are also available for planning and migration of large contact centers, and for integration of contact centers with cloud services including Salesforce.

Please explain how the State’s Telephony Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.
Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements

If an offeror needs to request a variance from a State IT Policy, Standard or Service requirement outlined in this supplement, please provide a rationale and an overview for each request in the table below.

<table>
<thead>
<tr>
<th>Section Reference</th>
<th>IT Policy, Standard or Service Requirement</th>
<th>Rationale for Proposed Variance from Requirement</th>
<th>Proposed Variance Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Example: The offeror shall use the State’s eSignature solution.</td>
<td>Example: An eSignature solution is already integrated into the proposed solution. Using the State’s service would result in increased cost due to integration complexities, as well as additional testing and resource needs. It would also result in longer deliverable timeframe.</td>
<td>Example: The Offeror’s eSignature solution provides the same capabilities as the State’s required solution. The Offeror’s solution includes a workflow component and an eSignature User interface.</td>
</tr>
</tbody>
</table>
State Information Security and Privacy Requirements

State Data Handling Requirements

Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/01/2019</td>
<td>Updated the State Information Security and Privacy Requirements as well as the State Data Handling Requirements to align with current practices.</td>
<td>1.0</td>
</tr>
</tbody>
</table>
# Table of Contents

State Information Security, Privacy and Data Handling Requirements Instructions ................................................................. 1
Overview and Scope .................................................................................................................................................................. 1

State Requirements Applying to All Solutions......................................................................................................................... 1

1. State Information Security and Privacy Standards and Requirements .............................................................................. 2
   1.1. The Offeror’s Responsibilities ........................................................................................................................................ 2
   1.2. The State’s Responsibilities ........................................................................................................................................... 3
   1.3. Periodic Security and Privacy Audits .............................................................................................................................. 3
       1.3.1. State Penetration and Controls Testing .................................................................................................................. 4
       1.3.2. System Security Plan ................................................................................................................................................. 4
       1.3.3. Risk Assessment ......................................................................................................................................................... 12
   1.4. Security and Data Protection ........................................................................................................................................ 12
   1.5. Protection of State Data .................................................................................................................................................. 13
   1.6. Handling the State’s Data ................................................................................................................................................ 14
   1.7. Contractor Access to State Networks Systems and Data .............................................................................................. 15
   1.8. State Network Access (VPN) .......................................................................................................................................... 17
   1.9. Portable Devices and Media ........................................................................................................................................... 17

2. State and Federal Data Privacy Requirements ...................................................................................................................... 18
   2.1. Contractor Requirements ............................................................................................................................................... 18
       2.2. Federal Tax Information (FTI) ..................................................................................................................................... 19
           2.2.1. IRS 1075 Performance Requirements .................................................................................................................. 19
           2.2.2. IRS 1075 Criminal/Civil Sanctions ....................................................................................................................... 20
           2.4.3. Disclosure ......................................................................................................................................................... 21
           2.5. Background Investigations of Contractor Personnel .......................................................................................... 22
   2.3. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues ........................................ 23
       3.1. General .................................................................................................................................................... 23
           3.2. Actual or Attempted Access or Disclosure ........................................................................................................ 23
           3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities .................................................................... 24
           3.4. Security Incident Reporting and Indemnification Requirements ........................................................................ 25
   4. Security Review Services ..................................................................................................................................................... 26
       4.1. Hardware and Software Assets ................................................................................................................................ 26
       4.2. Security Standards by Device and Access Type .................................................................................................. 27
       4.3. Boundary Defenses .................................................................................................................................................... 27
4.4. Audit Log Reviews ......................................................................................................................... 28
4.5. Application Software Security ..................................................................................................... 28
4.7. Account Access Privileges ........................................................................................................ 30
4.8. Additional Controls and Responsibilities ..................................................................................... 30
Appendix A – Compensating Controls to Security and Privacy Supplement ........................................ 32
State Information Security, Privacy and Data Handling Requirements Instructions

When providing a response to this Supplement, please follow the instructions below and frame your response as it relates to your proposed solution e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid.

1. After each specific requirement the offeror must provide a response on how the requirement will be met or indicate if it is not applicable and why.

2. In the event there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it in Appendix A – Compensating Controls to Security and Privacy Requirements. Please be sure to provide a rationale for the change.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Current Language</th>
<th>Contractor’s Proposed Change</th>
<th>Rationale of Proposed Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Example: Provide vulnerability management services for the Contractor’s internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State monthly.</td>
<td>Example: Provide vulnerability management services for the Contractor’s internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State weekly.</td>
<td>Per company policy vulnerability report are only provided to customers on a quarterly basis.</td>
</tr>
</tbody>
</table>

3. Upon completion, please submit the security supplement responses with the proposal documentation.
Overview and Scope

This supplement shall apply to the Contracts for all work, services, locations (e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid) along with the computing elements that the Contractor will perform, provide, occupy, or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with the delivery of work.

The selected Contractor will accept the security and privacy requirements outlined in this supplement in their entirety as they apply to the services being provided to the State. The Contractor will be responsible for maintaining information security in environments under the Contractor’s management and in accordance with State IT security policies and standards.

This scope shall specifically apply to:

- Major and minor projects, upgrades, updates, fixes, patches, and other software and systems inclusive of all State elements or elements under the Contractor’s responsibility utilized by the State.
- Any systems development, integration, operations, and maintenance activities performed by the Contractor.
- Any authorized change orders, change requests, statements of work, extensions, or amendments to this contract.
- Contractor locations, equipment, and personnel that access State systems, networks or data directly or indirectly.
- Any Contractor personnel or sub-contracted personnel that have access to State confidential, personal, financial, infrastructure details or sensitive data.

The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in this contract shall prevail.

Please note that any proposed compensating controls to the security and privacy requirements outlined in this supplement are required to be identified in Appendix A – Compensating Controls to Security and Privacy Requirements. Contractors are asked not to make any changes to the language contained within this supplement.

State Requirements Applying to All Solutions

This section describes the responsibilities for both the selected Contractor and the State of Ohio as it pertains to State information security and privacy standards and requirements for all proposed solutions whether cloud, on-premises, or hybrid based. The Contractor will comply with State of Ohio IT security and privacy policies and standards as they apply to the services being provided to the State. A list of IT policy and standard links is provided in the State IT Policy and Standard Requirements and State IT Service Requirements supplement.
1. **State Information Security and Privacy Standards and Requirements**

The Contractor is responsible for maintaining the security of information in accordance with State security policies and standards. If the State is providing the network layer, the Contractor must be responsible for maintaining the security of the information in environment elements that are accessed, utilized, developed, or managed. In either scenario, the Contractor must implement information security policies, standards, and capabilities as set forth in statements of work and adhere to State policies and use procedures in a manner that does not diminish established State capabilities and standards.

1.1. **The Offeror’s Responsibilities**

The offeror’s responsibilities with respect to security services include the following, where applicable:

1.1.1. Support State IT security policies and standards, which includes the development, maintenance, updates, and implementation of security procedures with the State’s review and approval, including physical access strategies and standards, User ID approval procedures, and a security incident action plan.

1.1.2. Support the implementation and compliance monitoring as per State IT security policies and standards.

1.1.3. If the Contractor identifies a potential issue with maintaining an “as provided” State infrastructure element in accordance with a more stringent State level security policy, the Contractor shall identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.

1.1.4. Support intrusion detection and prevention, including prompt State notification of such events and reporting, monitoring, and assessing security events.

1.1.5. Provide vulnerability management services for the Contractor’s internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. At a minimum, the Contractor shall provide vulnerability scan results to the State monthly.

1.1.6. Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a security incident response plan.

1.1.7. Manage and administer access to the systems, networks, system software, systems files, State data, and end users if applicable.

1.1.8. Install and maintain current versions of system software security, assign and reset passwords per established procedures, provide the State access to create User IDs, suspend and delete inactive User IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.

1.1.9. Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.

1.1.10. Perform physical security functions (e.g., identification badge controls and alarm responses) at the facilities under the Contractor’s control.
1.2 The State’s Responsibilities

The State will:

1.2.1. Develop, maintain, and update the State IT security policies, including applicable State information risk policies, standards, and procedures.

1.2.2. Provide the Contractor with contact information for security and program personnel for incident reporting purposes.

1.2.3. Provide a State resource to serve as a single point of contact, with responsibility for account security audits.

1.2.4. Support intrusion detection, prevention, and vulnerability scanning pursuant to State IT security policies.

1.2.5. Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.

1.2.6. Provide audit findings material for the services based upon the security policies, standards and practices in effect as of the effective date and any subsequent updates.

1.2.7. Assist the Contractor in performing a baseline inventory of User IDs for the systems for which the Contractor has security responsibility.

1.2.8. Authorize user IDs and passwords for State personnel for the system’s software, software tools and network infrastructure systems and devices under Contractor management.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

1.3 Periodic Security and Privacy Audits

The State will be responsible for conducting periodic security and privacy audits and will generally utilize members of the Office of Information Security and Privacy, the Office of Budget and Management – Office of Internal Audit, and the Auditor of State, depending on the focus area of the audit. Should an audit issue or finding be discovered, the following resolution path shall apply:

If a security or privacy issue exists in any of the IT resources furnished to the Contractor by the State (e.g., code, systems, computer hardware and software), the State will have responsibility to address or resolve the issue. The State may elect to work with the Contractor, under mutually agreeable terms for resolution services or the State may elect to address the issue independent of the Contractor. The Contractor is responsible for resolving any security or privacy issues that exist in any of the IT resources they provide to the State.
For in-scope environments and services, all new systems implemented or deployed by the Contractor must comply with State security and privacy policies and standards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.1. State Penetration and Controls Testing

The State may, at any time in its sole discretion, elect to perform a Security and Data Protection Audit. This includes a thorough review of Contractor controls, security/privacy functions and procedures, data storage and encryption methods, backup/restoration processes, as well as security penetration testing and validation. The State may utilize a third-party Contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met.

State acceptance testing will not proceed until the Contractor cures, according to the State’s written satisfaction, all findings, gaps, errors or omissions pertaining to the audit. Such testing will be scheduled with the Contractor at a mutually agreed upon time.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.2. System Security Plan

A completed System Security Plan must be provided by the Contractor to the State and the primary point of contact from the Office of Information Security and Privacy no later than the end of the project development phase of the System Development Life Cycle (SDLC). The plan must be updated annually or when major changes occur within the solution. The templates referenced below are the required format for submitting security plans to the State.
[Insert System Name Here]

System Security Plan

Security Categorization: [Level Here]

{DATE}

Version {x.x}

Prepared by:

Executive Summary

State of Ohio agencies are required to identify each information system that contains, processes, and transmits state data and information and to prepare and implement a plan for the security and privacy of these systems. The objective of system security planning is to improve protection of information technology (IT) resources. All State of Ohio systems have some level of sensitivity, and require protection as part of best management practices. The protection of a system must be documented in a system security plan.
The security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from management responsible for the system, including information owners, the system operator, the system security manager, and system administrators.

This System Security Plan (SSP) provides an overview of the security requirements for `<System Name>` and the associated controls document describes the controls in place or planned for implementation to provide a level of security appropriate for the information processed as of the date indicated.

Note: The SSP is a living document that will be updated periodically to incorporate new and/or modified security. The plan will be revised as the changes occur to the system, the data or the technical environment in which the system operates.

### Change/Review Record

This [Insert System Name Here] System Security Plan (SSP) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the Change/Review Record below. Reviews made as part of the assessment process should also be recorded below. This history shall be maintained throughout the life of the document.

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Description of Change/Revision</th>
<th>Section/Pages Affected</th>
<th>Changes Made by Name/Title/Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>[Insert Update Date Here]</td>
<td>Template Created</td>
<td>All</td>
<td>[Insert Name/Title/Team]</td>
</tr>
</tbody>
</table>
System Security Plan Approval Signatures

I have reviewed the [Insert System Name Here] System Security Plan and accept the analysis and findings within.

[Insert Name Here]  [Insert Name Here]  [Insert Date]
System Owner

1. Information System Name/Title:
   • Unique identifier and name given to the system.

2. Information System Categorization/Security Risks and Concerns:
   • To identify the information system categorization in reference with FIPS-199. The information gathered from the data classification and risk assessment will provide the details necessary to select the appropriate level.
3. Information System Owner:
   • Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official:
   • Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts:
   • List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility:
   • Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status:
   • Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

8. General System Description/Purpose
   • Describe the function or purpose of the system and the information processes.
9. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, communications equipment, infrastructure architecture, security processes.

- Detail the technical specifics to satisfy the following Network segmentation, Perimeter security, Application security and data sensitivity classification, PHI and PII data elements, Intrusion management, Monitoring and reporting, Host hardening, Remote access, Encryption, State-wide active directory services for authentication, Interface security, Security test procedures, Managing network security devices, Security patch management, Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls and Secure communications over the Internet.
10. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Organization</th>
<th>Type</th>
<th>Agreement (ISA/MOU/MOA)</th>
<th>Date of Agreement</th>
<th>Categorization Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11. Related Laws/Regulations/Policies/Guidelines
   • List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

Please provide a controls document with the appropriate selection of a minimum or in place security control baseline based on the system categorization (low, moderate, and high-impact) or tailored controls in the organizations framework format (NIST SP 800-53, ISO27001, COBIT, etc.).

The document must contain a thorough description of how all the minimum or in place security controls within the applicable baseline or control tailoring are being implemented or planned to be implemented.

The description should contain:
   • Security control title
   • How the security control is being implemented or planned to be implemented.
   • Any scoping guidance that has been applied and what type of consideration.
   • Indicate if the security control is a common control and who is responsible for its implementation.
   • Logical security controls (privacy, user access and authentication, user permissions, etc.)
   • Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)

13. Information System Security Plan Completion Date: _____________________
   • Enter the completion date of the plan.

14. Information System Security Plan Approval Date: _____________________
   • Enter the date the system security plan was approved by the system owner and indicate if the approval documentation is attached or on file.
15. Security System/Project Deliverables

- Enter Please list the security specific project deliverables within this section.

16. Attachment (A) – Security Controls Document

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.3. Risk Assessment

A Risk Assessment report completed within the past 12 months must be provided to the State and the primary point of contact from the Office of Information Security and Privacy no later than the project development phase of the System Development Life Cycle (SDLC). A new risk assessment must be conducted every two years, or as a result of significant changes to infrastructure, a system or application environment, or following a significant security incident.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.4. Security and Data Protection

All solutions must classify data per State of Ohio IT-13 Data Classification policy and per the sensitivity and criticality, must operate at the appropriate baseline (low, moderate, high) as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Security and Privacy Controls for Federal
Information Systems and Organizations” (current, published version), be consistent with Federal Information Security Management Act (“FISMA 2014”) requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. The solution must provide the State’s systems administrators with 24x7 visibility into the services through a real-time web-based “dashboard” capability that enables them to monitor, in real or near real time, the services’ performance against the established service level agreements and promised operational parameters.

If the solution is cloud based, the Contractor must obtain an annual audit that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (“SSAE”) No. 16, Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2. The audit must cover all operations pertaining to the Services covered by this Agreement. The audit will be at the sole expense of the Contractor and the results must be provided to the State within 30 days of its completion each year.

At no cost to the State, the Contractor must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the Services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.5. Data

1.5.1. “State Data” includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.

1.5.2. “Sensitive Data” is any type of data that presents a high or moderate degree of risk if released or disclosed without authorization. Sensitive Data includes but not limited to:

1.5.2.1. Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.

1.5.2.2. Federal Tax Information (FTI) under IRS Special Publication 1075,

1.5.2.3. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA)

1.5.2.4. Criminal Justice Information (CJI) under Federal Bureau of Investigation’s Criminal Justice Information Services (CJIS) Security Policy.

1.5.2.5. The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.
1.6. Protection and Handling the State’s Data

To protect State Data as described in this contract, the Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect State Data from unauthorized disclosure, modification, use or destruction.

To accomplish this, the Contractor must adhere to the following requirements regarding State Data:

1.6.1. Maintain in confidence State Data it may obtain, maintain, process, or otherwise receive from or through the State in the course of the contract.

1.6.2. Use and permit its employees, officers, agents, and subcontractors to use any State Data received from the State solely for those purposes expressly contemplated by the contract.

1.6.3. Not sell, rent, lease, disclose, or permit its employees, officers, agents, and sub-contractors to sell, rent, lease, or disclose, any such State Data to any third party, except as permitted under this contract or required by applicable law, regulation, or court order.

1.6.4. Take all commercially reasonable steps to (a) protect the confidentiality of State Data received from the State and (b) establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to State Data received by the Contractor from the State.

1.6.5. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.

1.6.6. Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of State Data.

1.6.7. Align with existing State Data security policies, standards and procedures designed to ensure the following:

   1.6.7.1. Security and confidentiality of State Data

   1.6.7.2. Protection against anticipated threats or hazards to the security or integrity of State Data

   1.6.7.3. Protection against the unauthorized access to, disclosure of, or use of State Data

1.6.8. Suggest and develop modifications to existing data security policies and procedures or draft new data security policies and procedures when gaps are identified.

1.6.9. Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.

1.6.10. Give access to State Data only to those individual employees, officers, agents, and sub-contractors who reasonably require access to such information in connection with the performance of Contractor’s obligations under this contract.

1.6.11. Maintain appropriate identification and authentication processes for information systems and services associated with State Data.
1.6.12. Any Sensitive Data at rest, transmitted over a network, or taken off-site via portable/removable media must be encrypted pursuant to the State’s data encryption standard, Ohio IT Standard ITS-SEC-01, “Data Encryption and Cryptography,” and Ohio Administrative Policy IT-14, “Data Encryption and Securing State Data.”

1.6.13. Any data encryption requirement identified in this supplement means encryption that complies with National Institute of Standards and Technology’s Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number.

1.6.14. Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.

1.6.15. Implement and manage security audit logging on information systems, including computers and network devices.

1.6.16. Cooperate with any attempt by the State to monitor Contractor’s compliance with the foregoing obligations as reasonably requested by the State. The State will be responsible for all costs incurred by the Contractor for compliance with this provision of this subsection.

1.6.17 Upon request by the State, promptly destroy or return to the State, in a format designated by the State, all State Data received from or through the State.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.7. **Contractor Access to State Network Systems and Data**

The Contractor must maintain a robust boundary security capability that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these ports, and disabling all others.

To do this, the Contractor must:

1.7.1 Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.

1.7.2 Use multifactor authentication to limit access to systems that contain Sensitive Data, such as Personally Identifiable Information.
1.7.3. Assume all State Data is both confidential and critical for State operations. The Contractor's security policies, plans, and procedures for the handling, storage, backup, access, and, if appropriate, destruction of State Data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.

1.7.4. Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data, as well as attacks on the Contractor's infrastructure associated with the State Data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State Data.

1.7.5. Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State data is stored. The method of securing the State Data must be in alignment with the required data classification and risk assessment outcomes, and may include secure overwriting, destruction, or encryption of the State data before transfer of control in alignment with NIST SP 800-88. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this contract.

1.7.6. Have a business continuity plan in place that the Contractor tests and updates no less than annually. The plan must address procedures for responses to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains State Data in case of loss of State Data at the primary site. The Contractor’s backup solution must include plans to recover from an intentional deletion attempt by a remote attacker exploiting compromised administrator credentials. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State Data in the case of a disaster or other business interruption. The Contractor’s business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the Sensitive Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

1.7.7. Not allow State Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this contract. If necessary, for such performance, the Contractor may permit State Data to be loaded onto portable computing devices or portable storage components or media only if adequate security measures are in place to ensure the integrity and security of State Data. Those measures must include a policy on physical security and appropriate encryption for such devices to minimize the risk of theft and unauthorized access as well as a prohibition against viewing sensitive or confidential data in public or common areas.

1.7.8. Ensure that portable computing devices have anti-virus software, personal firewalls, and system password protection. In addition, State Data must be encrypted when stored on any portable computing or storage device or media or when transmitted across any data network.

1.7.9. Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.
1.8. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including transport layer security (TLS) and public key authentication, signing and/or encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided public key infrastructure (PKI). Multifactor authentication must be employed for users with privileged network access by State provided solutions.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.9. Portable Devices and Media

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such devices to the State in writing as defined in Section 3 Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues. The Contractor must have a written policy that defines procedures for how the Contractor must detect, evaluate, and respond to adverse events that may indicate an incident or an attempt to attack or access State Data or the infrastructure associated with State Data.
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2. State and Federal Data Privacy Requirements

All systems and services must be designed and must function according to Fair Information Practice Principles (FIPPS), which are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability, and auditing.

To the extent that personally identifiable information (PII) in a system is “protected health information” under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the FIPPS principles must be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in a system that is not “protected health information” under HIPAA, the FIPPS principles must still be implemented and, when applicable, aligned to other laws or regulations.

2.1 Contractor Requirements

The Contractor specifically agrees to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to the work associated with this Contract including but not limited to:


2.1.3. Ohio Revised Code (ORC) 1347.01, 1347.04 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5160.39, 5168.13, and 5165.88.

2.1.4. Corresponding Ohio Administrative Code Rules and Updates.

2.1.5. Systems and services must support and comply with the State’s security operational support model, which is aligned to NIST SP 800-53 (current, published version).

2.1.6. IRS Publication 1075, Tax Information Security Guidelines for federal, state, and local agencies.

2.1.7. Criminal Justice Information Systems Policy.
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.2. Federal Tax Information (FTI)

All computer systems receiving, processing, storing, or transmitting Federal Tax Information (FTI) must meet the requirements defined in IRS Publication 1075.

2.2.1. IRS 1075 Performance Requirements:

In the performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

2.2.1.1. All work involving FTI will be done under the supervision of the Contractor or the Contractor's employees.

2.2.1.2. The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

2.2.1.3. Any federal tax return or return information made available in any format shall be used only for the purposes of performing this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the Contractor is prohibited.

2.2.1.4. All federal tax returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

2.2.1.5. The Contractor certifies that the IRS data processed during the performance of this contract will be completely purged from all data storage components of its computer facility, and no output will be retained by the Contractor after the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosure.

2.2.1.6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the State or its designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the State or its designee with a Statement containing the date of destruction, description of material destroyed, and the method used.

2.2.1.7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in the IRS Publication 1075. To meet functional and assurance requirements, the security
features of the environment must provide for the managerial, operations, and technical IRS 1075 controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

2.2.1.8 No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

2.2.1.9. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

The agency will have the right to void the Contract if Contractor fails to provide the safeguards described above.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.2.2. IRS 1075 Criminal/Civil Sanctions

2.2.2.1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

2.2.2.2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.
2.2.2.3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

2.2.3. **Inspection**

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor for inspection of the facilities and operations performing any work under this contract for compliance with requirements defined in IRS Publication 1075. The IRS’ right of inspection shall include the use of manual, and/or automated scanning tools to perform compliance and vulnerability assessment of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with contract safeguards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.3. **Disclosure**

**Disclosure to Third Parties.** This Contract must not be deemed to prohibit disclosures in the following cases:

2.3.1. Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether Sensitive Data or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule or regulation, Contractor must notify the State within 24 hours in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor must also cooperate in the State’s efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor must advise and consult with the State and its counsel as to the scope of such disclosure and the nature of wording of such disclosure) and Contractor must use commercially reasonable efforts to obtain confidential treatment for the information:

2.3.1.1. To State auditors or regulators.
2.3.1.2. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations.

2.3.1.3. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.4. **Background Investigations of Contractor Personnel**

Contractor agrees that (1) the State of Ohio will conduct background investigations on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no ineligible personnel will perform Sensitive Services under this contract. The term “ineligible personnel” means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (c) has been convicted of a felony.

“Sensitive Services” means those services that (i) require access to customer, consumer, or State employee information, (ii) relate to the State’s computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities.

Contractors who will have access to Federal Tax Information (FTI) or Criminal Justice Information (CJI) must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information. In addition, existing Contractors with access to FTI or CJI that have not completed a background investigation within the last 5 years must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information.

FTI or criminal justice background investigations will include:

2.4.1. FBI Fingerprinting (FD-258)

2.4.2. Local law enforcement agencies where the employee has lived, worked and/or attended school within the last five years

2.4.3. Citizenship/residency eligibility to legally work in the United States

2.4.4. New employees must complete USCIS Form I-9, which must be processed through the Federal E-Verify system

2.4.5. FTI training, with a 45 day wait period
In the event that the Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3. Contractor Responsibilities Related to Reporting of Concerns, Issues, and Security/Privacy Issues

3.1. General

If, over the course of the Contract a security or privacy issue arises, whether detected by the State, a State auditor, or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any contracted service associated with this Contract, the Contractor must:

3.1.1. Notify the State of the issue or acknowledge receipt of the issue within two (2) hours.

3.1.2. Within forty-eight (48) hours from the initial detection or communication of the issue from the State, present a potential exposure or issue assessment document to the State account representative and the State Chief Information Security Officer with a high-level assessment as to resolution actions and a plan.

3.1.3. Within four (4) calendar days, and upon direction from the State, implement, to the extent commercially reasonable, measures to minimize the State’s exposure to the security or privacy issue until such time as the issue is resolved.

3.1.4. Upon approval from the State, implement a permanent repair to the identified issue at the Contractor’s cost.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.2. Actual or Attempted Access or Disclosure
If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any Sensitive Data by the Contractor or any of its Subcontractors (collectively “Disclosure”) and/or any unauthorized intrusions into Contractor’s or any of its Subcontractor’s facilities or secure systems (collectively “Intrusion”), Contractor must immediately:

3.2.1. Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized disclosure or intrusion.

3.2.2. Investigate and determine if an intrusion and/or disclosure has occurred.

3.2.3. Fully cooperate with the State in estimating the effect of the disclosure or intrusion and fully cooperate to mitigate the consequences of the disclosure or intrusion.

3.2.4. Specify corrective action to be taken.

3.2.5. Take corrective action to prevent further disclosure and/or intrusion.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

The following are the responsibility of the Contractor to provide at its own cost:

3.3.1. The Contractor must, as soon as is practical, make a report to the State including details of the disclosure and/or intrusion and the corrective action the Contractor has taken to prevent further disclosure and/or intrusion. The Contractor must, in the case of a disclosure, cooperate fully with the State to notify the affected persons as to the facts and circumstances of the disclosure of the Sensitive Data. Additionally, the Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies that have jurisdiction to investigate a disclosure and/or any known or suspected criminal activity.

3.3.2. If, over the course of delivering services to the State under this statement of work for in-scope environments, the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams, the Contractor must notify the State within two (2) hours. This notification must not minimize the more stringent service level contracts pertaining to security scans and breaches contained herein, which due to the nature of an active breach must take precedence over this notification. The State may elect to work with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

3.3.3. If the Contractor identifies a potential issue with maintaining an “as provided” State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies.
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.4. Security Incident Reporting and Indemnification Requirements

3.4.1. The Contractor must report any security incident of which it becomes aware. For the purposes of this document, “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It does not mean unsuccessful log-on attempts, denial of service attacks, unsuccessful network attacks such as pings, probes of firewalls, port scans, or any combination of those, as long as there is no unauthorized access, acquisition, use, or disclosure of Sensitive Data as a result.

3.4.2. In the case of an actual security incident that may have compromised Sensitive Data, the Contractor must notify the State in writing within two (2) hours of the Contractor becoming aware of the breach. The Contractor is required to provide the best available information from the investigation.

3.4.3. In the case of a suspected incident, the Contractor must notify the State in writing within twenty-four (24) hours of the Contractor becoming aware of the suspected incident. The Contractor is required to provide the best available information from the investigation.

3.4.4. The Contractor must fully cooperate with the State to mitigate the consequences of an incident/suspected incident at the Contractor’s own Cost. This includes any use or disclosure of the Sensitive Data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this contract by an employee, agent, or Subcontractor of the Contractor.

3.4.5. The Contractor must give the State full access to the details of the breach/suspected breach and assist the State in making any notifications to potentially affected people and organizations that the State deems necessary or appropriate at the Contractor’s own cost.

3.4.6. The Contractor must document and provide incident reports for all such incidents/suspected incidents to the State. The Contractor must provide updates to incident reports until the investigation is complete at the Contractor’s own cost. At a minimum, the incident/suspected incident reports will include:

3.4.6.1. Data elements involved, the extent of the Data involved in the incident, and the identification of affected individuals, if applicable.

3.4.6.2. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed State Data, or to have been responsible for the incident.
3.4.6.3. A description of where the State Data is believed to have been improperly transmitted, sent, or utilized, if applicable.

3.4.6.4. A description of the probable causes of the incident.

3.4.6.5. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval.

3.4.6.6. Whether the Contractor believes any federal or state laws requiring notifications to individuals are triggered.

3.4.7. In addition to any other liability under this contract related to the Contractor’s improper disclosure of State Data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year’s identity theft protection service on behalf of any individual or entity whose Sensitive Data is compromised while it is in the Contractor’s possession. This service will be provided at Contractor’s own cost. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individual’s credit history through those services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

4.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this includes:

4.1.1. Deviations from the hardware baseline.

4.1.2. Inventory of information types by hardware device.

4.1.3. Software inventory compared against licenses (State purchased).

4.1.4. Software versions and then scans of versions against patches distributed and applied.
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

### 4.2. Security Standards by Device and Access Type

The Contractor must:

4.2.1. Document security standards by device type and execute regular scans against these standards to produce exception reports.

4.2.2. Document and implement a process for any required remediation.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

### 4.3. Boundary Defenses

The Contractor must:

4.3.1. Work with the State to support the denial of communications to/from known malicious IP addresses.

4.3.2. Ensure that the system network architecture separates internal systems from DMZ and extranet systems.

4.3.3. Require the use of two-factor authentication for remote login.

4.3.4. Support the State’s monitoring and management of devices remotely logging into the internal network.

4.3.5. Support the State in the configuration of firewall session tracking mechanisms for addresses that access the solution.
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.4. Audit Log Reviews

The Contractor must:

4.4.1. Work with the State to review and validate audit log settings for hardware and software.

4.4.2. Ensure that all systems and environments have adequate space to store logs.

4.4.3. Work with the State to devise and implement profiles of common events from given systems to reduce false positives and rapidly identify active access.

4.4.4. Provide requirements to the State to configure operating systems to log access control events.

4.4.5. Design and execute bi-weekly reports to identify anomalies in system logs.

4.4.6. Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.5. Application Software Security

The Contractor must:

4.5.1. Perform configuration review of operating system, application, and database settings.

4.5.2. Ensure software development personnel receive training in writing secure code.
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A – Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

**4.6. System Administrator Access**

The Contractor must:

4.6.1. Inventory all administrative passwords (application, database, and operating system level).

4.6.2. Implement policies to change default passwords in accordance with State policies, following any transfer or termination of personnel (State, existing Materials and Supplies Vendor, or Contractor).

4.6.3. Configure administrative accounts to require regular password changes.

4.6.4. Ensure user and service level accounts have cryptographically strong passwords.

4.6.5. Store passwords in a hashed or encrypted format.

4.6.6. Ensure administrative accounts are used only for administrative activities.

4.6.7. Implement focused auditing of administrative privileged functions.

4.6.8. Configure systems to log entry and alert when administrative accounts are modified.

4.6.9. Segregate administrator accounts based on defined roles.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.
4.7. **Account Access Privileges**

The Contractor must, in alignment with policy requirements:

4.7.1. Review and disable accounts not associated with a business process.

4.7.2. Create a daily report that includes locked out accounts, disabled accounts, etc.

4.7.3. Implement a process for revoking system access.

4.7.4. Automatically log off users after a standard period of inactivity.

4.7.5. Monitor account usage to determine dormant accounts.

4.7.6. Monitor access attempts to deactivated accounts through audit logging.

4.7.7. Profile typical account usage and implement or maintain profiles to ensure that security profiles are implemented correctly and consistently.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.8. **Additional Controls and Responsibilities**

The Contractor must meet with the State no less frequently than annually to:

4.8.1. Review, update and conduct security training for personnel, based on roles.

4.8.2. Review the adequacy of physical and environmental controls.

4.8.3. Verify the encryption of Sensitive Data in transit.

4.8.4. Review access controls based on established roles and access profiles.

4.8.5. Update and review system administration documentation.

4.8.6. Update and review system maintenance policies.

4.8.7. Update and review system and integrity policies.

4.8.9. Review and implement updates to the System security plan.
4.8.10 Update risk assessment policies and procedures.

4.8.11 Update and implement incident response procedures.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.
## Appendix A – Compensating Controls to Security and Privacy Supplement

In the event that there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it below and provide a proposed language change as well as a rationale for the change.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Current Language</th>
<th>Contractor's Proposed Change</th>
<th>Rationale of Proposed Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><strong>Example:</strong> Provide vulnerability management services for the Contractor’s internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State <em>monthly</em>.</td>
<td><strong>Example:</strong> Provide vulnerability management services for the Contractor’s internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State <em>weekly</em>.</td>
<td>Per company policy vulnerability report are only provided to customers on a quarterly basis.</td>
</tr>
</tbody>
</table>