CITY OF COLUMBIA, MO
TRANSIT INTELLIGENT TRANSPORTATION SYSTEMS (ITS)
SOFTWARE AGREEMENT

THIS AGREEMENT (hereinafter "Agreement") is by and between the **City of Columbia, Missouri** (hereinafter "City"), a municipal corporation, and **ETA Phi Systems, Inc.** (hereinafter "Contractor"), a corporation with the authority to transact business within the State of Missouri, and is entered into on the date of the last signatory below (hereinafter "Effective Date"). City and Contractor are each individually referred to herein as a "Party" and collectively as the "Parties."

WITNESSETH:

WHEREAS, City is the owner and operator of a public transit system, Go COMO Transit, and has need for an intelligent transportation system (ITS) and associated services for automatic vehicle location to allow staff and the public to track buses along their routes through internal services and an external app available to the public, make audible announcements of bus stops, make public service announcements and provide service alerts, as well as other features provided for herein;

WHEREAS, Contractor submitted a proposal and pricing response to meet City's needs for such services; and

WHEREAS, City wishes to purchase, and Contractor wishes to provide, intelligent transportation system software services pursuant to the terms and conditions set forth herein.

NOW, THEREFORE, in consideration of the mutual covenants set out in this Agreement and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged), the Parties agree as follows:

1. CONTRACT DOCUMENTS. The Contract Documents include this Agreement and the following attachments and exhibits, which are incorporated herein by reference:

Exhibit:

A	Contractor's Response to City RFP 128/2023
B	Contractor Pricing Page

In the event of a conflict between the terms of any of the Contract Documents and the terms of this Agreement, the terms of this Agreement control.

2. PROJECT, STANDARDS AND SPECIFICATIONS AND TIMING.

a. The Project shall consist of all software, hardware and services necessary for complete implementation and use of the systems, as set forth more fully in the Contract Documents.

b. Contractor shall be responsible for, and agrees to perform, all work and services according to the specifications, material standards, procedures and quality standards set out in the Contract Documents.

c. *Timing of Work*. Contractor shall start work promptly, after receipt of a Notice to Proceed, and shall complete Phases of the Project as set forth in the Contract Documents, unless otherwise agreed to in writing by the Parties.

d. *Material and Workmanship*. All materials provided by Contractor shall be new materials of high quality which shall give long life and reliable operation. All equipment shall be modern in design and shall not have been in prior service except as required by factory tests. The workmanship shall be of high quality in every detail.

e. *Repairs and/or Replacement of Defective Portions*. Contractor shall be responsible for a period of five (5) years from and after the date of final acceptance by the City of the work covered by this Contract, for any repairs or replacements caused by defective materials, workmanship, or equipment which, in the judgment of the City, shall become necessary during such period. Contractor shall undertake with due diligence to make the aforesaid repairs and/or replacements within thirty (30) days after receiving written notice that such repairs or replacements are necessary. If Contractor should neglect to begin such repairs or replacements within this period, or, in case of emergency, where in the judgment of the City, delay would cause serious loss or damage, the repairs and/or replacements may be made by the City and charged to Contractor.

3. PAYMENT

a. *Pricing*. For the initial five (5) year term of this Agreement, both Parties agree the price for the Project will be set at the amounts provided in the Contractor's Pricing Page, attached hereto as Exhibit B. After the initial term, Contractor's fees may increase as provided in this Agreement. Any fee increase more than five percent (5%) shall require a contract amendment.

b. *Billing*. Contractor shall invoice the City in writing in a manner consistent with the Milestone Schedule, attached hereto in Exhibit A, based on the services that have been rendered and at prices consistent with the pricing provided for this Agreement.

c. *Payments*. City agrees to pay all uncontested amounts of the invoice within thirty (30) days of receipt of an invoice. City expressly reserves the right to disapprove in whole or in part a request for payment where the services rendered are not performed in a timely or satisfactory manner. If an amount of invoice is contested, then City shall notify Contractor in writing within twenty (20) days of receipt of the invoice. Within this written notice, City shall provide the reasoning for City's

disapproval. Contractor shall either (a) respond to the City's notice to contest in writing justifying its position, or (b) exercise due diligence in curing the issue raised. If a cure cannot be reached, then the Parties may mutually reach an agreement as to an acceptable alternative.

d. *Not to Exceed Amount*. For the initial five (5) year term, it is expressly understood by both Parties that in no event shall the cumulative amount of payment from City to Contractor exceed **Three Hundred Thirty Thousand Dollars ($330,000)**, unless otherwise agreed to by both Parties in writing and executed as an amendment to this Agreement. After the initial five year term, City will make payments in accordance with the terms and conditions of this Agreement.

4. TERM. The "Term" of this Agreement shall commence on the Effective Date and shall continue until the date that is five (5) years following the Effective Date, unless sooner terminated in accordance with the terms hereof. Thereafter, the Agreement shall automatically be renewed for successive terms of one (1) year (each successive term shall be called "Maintenance Term"), unless the Agreement is terminated pursuant to the provisions of this Agreement. The Agreement shall automatically terminate fifteen (15) years after Effective Date.

5. TERMINATION.

a. *Termination by Mutual Agreement*. Termination of the Agreement can be made at the mutual Agreement of both Contractor and City.

b. *Termination for Convenience*. City is entitled to terminate this Agreement for convenience, provided that the City provides sixty (60) days advance notice to Contractor of its intent to terminate. In such event, Contractor shall immediately stop work and City shall not be liable to Contractor except for payment of actual work performed prior to such notice. Anticipatory profits and consequential damages shall not be recoverable by Contractor.

c. *Termination upon Default*. Upon the occurrence of an event of Default, the non-Defaulting Party shall be entitled to immediately terminate this Agreement. A Party shall be considered in Default of this Agreement upon:

(i) A failure by a Party to pay any amount due hereunder, where such failure is not cured within thirty (30) days after written notice from the other Party of such failure to pay; or

(ii) Either Party has (a) commenced a voluntary case under any bankruptcy law, applied for or consented to the appointment of, or the taking of possession by, a receiver, trustee, assignee, custodian or liquidator of all or a substantial part of its assets, (b) failed, or admitted in writing its inability generally, to pay its debts as such debts become due, (c) made a general assignment for the benefit of creditors, (d) been adjudicated bankrupt or has filed a petition or an answer seeking an arrangement with creditors, (e) taken

advantage of any insolvency law or shall have submitted an answer admitting the material allegations of a petition in bankruptcy or insolvency proceeding, (f) become subject to an order, judgment or decree for relief, entered in an involuntary case, without the application, approval or consent of such Party any court of competent jurisdiction appointing a receiver, trustee, assignee, custodian or liquidator, for a substantial part of any of its assets and such order, judgment or decree shall continue unstayed and in effect for any period of one hundred eighty (180) consecutive days, (g) filed a voluntary petition in bankruptcy, (h) failed to remove an involuntary petition in bankruptcy filed against it within one hundred eighty (180) days of the filing thereof, or (i) become subject to an order for relief under the provisions of the United States Bankruptcy Act, 1 1 U.S.C. § 301; or

(iii) Any Party's actual fraud or other material misconduct in connection with this Agreement or the performance of its obligations under this Agreement; or

(iv) Any other default that has a material adverse effect on the non-defaulting Party if such default has not been cured by the defaulting Party within thirty (30) days after receiving written notice from the non-defaulting Party setting forth, in reasonable detail, the nature of such default and its impact on the non-defaulting Party; provided, however, that, in the case of any such default that is not reasonably capable of being cured within the 30-day cure period, the defaulting Party shall have additional time as necessary to cure the default if it commences to cure the default within such 30-day cure period and it diligently and continuously pursues such cure.

(v) The purported assignment of this Agreement in a manner inconsistent with the terms of this Agreement.

d. Upon the occurrence of an Event of Default by a Party, the non-defaulting Party shall have the following rights:

(i) To terminate this Agreement by providing at least sixty (60) days prior written notice to the other Party of its intent to exercise its termination rights, unless such Event of Default is cured prior to the date of termination;

(jj) To suspend performance of its obligations and duties hereunder immediately upon delivering written notice to the defaulting Party of its intent to exercise its suspension rights; and

(iii) To pursue any other remedy given under this Agreement or now or hereafter existing at law or in equity or otherwise.

6. DATA OWNERSHIP AND STORAGE. Contractor does not own any data obtained or gathered by or through the City's use of the Software and Services and any information derived therefrom. Contractor shall not sell, give away, or transfer any

personal customer data obtained by Contractor through the use of these systems by City. Contractor covenants that any data from the City, its employees or those persons or entities using the City's transit system through the use of the software, or derived therefrom shall be stored in the United States of America. The data or any information derived therefrom shall not be transferred, moved, or stored to or at any location outside the United States of America. All such data and any information derived therefrom shall be confidential and proprietary information belonging to either the City or its transit customers. Contractor shall not sell or give away any such City or customer data or information derived therefrom.

a. Contractor retains control over design elements of the user interface, including but not limited to elements such as bus and stop icons, map colors, banners, point of interest identification, and other related elements.

b. Contractor may use information in order to enhance the user experience. Information may be used in a manner specified by future agreements for platforms that will be jointly agreed upon by the Contractor and City.

c. Contractor will only use information once it has:

(i) Received permission from customer for such uses

(ii) Removed any personally identifying data

All information is owned by the City or its transit customers, and Contractor agrees not to sell or transfer any City or personal customer data.

7. LICENSING, WARRANTY, MAINTENANCE, SUBSCRIPTIONS and CLOUD HOSTING.

a. *Licensing*. Contractor hereby sells and licenses to City and City agrees to purchase and license from Contractor for City's purposes perpetual, site licenses for all the Software included in Attachment D. Contractor hereby grants to City any and all licenses needed for Project as set forth in the Contract Documents.

b. *Maintenance, Subscriptions and Cloud Hosting Services*. The Parties agree that City is paying for five years of maintenance, subscriptions and cloud hosting services during the initial Term. During any Maintenance Term, Contractor's standard fees associated with maintenance, subscriptions, and cloud hosting may increase or decrease. Contractor agrees to provide City with pricing for maintenance, subscriptions, and cloud hosting at the lowest rate offered to Contractor's customers. Any fee increase of more than five percent (5%) shall require a contract amendment.

c. *Warranties and Maintenance*. The Contractor warrants that all components provided under this Agreement shall be: newly manufactured equipment or assembled from newly manufactured parts; approved by Underwriter's Laboratories; and, will be free from defects in workmanship or material for a period of five (5) years

from the date of final system acceptance. During the five (5) year warranty period, the Contractor shall furnish all replacement new parts, shipping costs, repaired parts, service labor, travel costs, and other repair costs at no cost to the City.

1. Third party software. Contractor warrants that all third party software products, brands, types, etc., have been recommended based on Contractor's understanding of the City's operating environment and that such third party software products, brands, types, etc., shall operate as demonstrated by and documented or represented by Contractor. Contractor further warrants that Contractor has the right to license said third party software products, brands, types, etc.

2. Third party hardware. Any and all hardware products, brands, types, etc., that Contractor provides to City pursuant to this Agreement shall be warranted to perform satisfactorily (defined as minimum ninety eight percent (98%) uptime during normal business hours and maximum three (3) second response time to non-query commands) for five (5) years from the signing of this Agreement, assuming local or other hardware support contracts are in effect for routine maintenance and diagnostics.

3. Warranty of Fitness for a Particular Purpose. Given City's documentation about the City's particular purpose, the Contractor acknowledges at the time this Agreement is in force that Contractor has (1) reason and opportunity to know the particular purpose for which products are required, and (2) that the City is relying on the Contractor's experience and knowledge of these products to provide those which are most suitable and appropriate. Therefore, the Contractor warrants that the system is fit for the purposes for which it is intended as described in this Agreement.

4. Resolution and Response Time Warranty. Contractor warrants that all Resolution and Response Times delineated below shall be adhered to as follows:

a. Priority 1 support issues are defined as: Mission Critical — Software is down [undiagnosed but feared critical; situation may require a restore and Software use is suspended until a diagnosis is given.

(i) Response to first call time limit — within two (2) business hours

(ii) Resolution time limit — CONTRACTOR shall use its best efforts to resolve within one (1) business day

(iii) If Contractor and City are on a support telephone call to resolve a Priority 1 support issue at the time that normal support hours end, Contractor support representatives will remain on the call past the normal support hours to provide what assistance can be provided at no additional

cost. City acknowledges that programmers will not be available at that time.

Penalty for not adhering to time limits - City shall receive a one percent (1%) credit against the annual Support fees, per incident, with a maximum of three (3) incidents or three percent (3%) reduction in any one year.

b. Priority 2 support issues are defined as: Critical Issue — Software is not down, but operations are negatively impacted.

(i) Response to first call time limit — within four business hours

(ii) Resolution time limit — Contractor shall use its best efforts to resolve within one (1) business week

(iii) Penalty for not adhering to time limits - City shall receive a one percent (1%) credit against the annual Support fees, per incident, with a maximum of three (3) incidents or three percent (3%) reduction in any one (1) year.

c. Priority 3 support issues are defined as: Non-Critical Issue — resolution period to be mutually agreed upon.

(i) Response to first call time limit — within twenty-four (24) business hours

(ii) Resolution time limit — Contractor shall use its best efforts to resolve within one (1) business week.

(iii) Penalty for not adhering to time limits - City shall receive a one percent (1%) credit against the annual Support fees, per incident, with a maximum of three (3) incidents or three percent (3%) reduction in any one (1) year.

d. Continuity of Warranty. City may continue the Warranty protection described above by purchasing and paying for on-going Annual Support services described below during the Maintenance Terms. By doing so, all Warranty, Warranty of Fitness for a Particular Use, and Resolution and Response Time Warranty conditions above shall remain in effect, in perpetuity (except for the "Third party hardware" clause above), as long as payments for Annual Support are kept current.

e. Final Acceptance of the System. The City will consider the system finally accepted upon successful completion of equipment installation, training, system testing, and receipt of as-built documentation in accordance with the terms of this Agreement. The City's final acceptance shall not be unreasonably withheld upon meeting all acceptance criteria.

8. UPGRADES TO SOFTWARE. City is entitled to receive any maintenance updates to the Service that Contractor may release or provide to its other customers that improves or maintains the stability of the Service ("Updates") at no cost to Customer. If new features that add new functionality to the Service ("Upgrades") are offered for sale to Contractor's other customers, such features will be offered to Customer at or below the prevailing rate. In the case where Contractor provides new features to Customer at no charge for testing or trial, the continued availability, performance, or usefulness of such features are not guaranteed or warranted by Contractor and such features may be revoked at any time. Contractor reserves the right to charge for any significant additional data requests made by the City over the course of the contract, including but not limited to bus number changes, route changes, and related additions, deletions, or alterations to system data.

9. SUNSHINE LAW. Access to data shall be granted in accordance with Missouri's open records law. The City of Columbia Public Works Department Records Custodian shall serve as the custodian of records for open records requests. Contractor shall provide access, at no additional costs, to the City of Columbia Public Works Department records custodian or his or her designee to all City's data and the data to allow for the fulfillment of Sunshine requests. Contractor shall provide all reasonable requests for information free of charge, including records and contracts data. Contractor reserves the right to charge City for any data requests which present a burden on business operations, including access to database information.

10. RECORDS RETENTION.

a. Pursuant to Missouri Law, both Parties agree that all records shall be retained in accordance with Missouri law and records retention schedules adopted by the Local Records Board and in accordance with the requirements of the Federal Grant. If there is a conflict between Missouri Law, then applicable retention schedule adopted by the Local Records Board, and the Grant requirements, the longer retention period shall apply.

b. *Effect of Termination and Records Retention*. At the close date for this Agreement, either through contract duration or termination, Contractor shall provide City with all records as defined by law. Contractor shall provide to City at no cost a method of migrating or exporting all electronic records or data in a usable basis in a method and format acceptable to City. At City's sole option, City may choose to negotiate a new contract for ongoing storage and access to all City records and data as needed to comply with the Missouri Sunshine Law and the record retention requirements of the Grant or as required by law.

11. DEVELOPMENT OF ADDITIONAL APPLICATIONS USING DATA.

a. Contractor shall provide access to data through an API to allow City to develop additional applications using the data, to hire others to develop additional applications, to allow members of the public to develop additional applications, including but not limited to work for hire or a contest type event. Contractor shall provide access to data to allow any such applications to utilize real time transit data.

b. *Notice of Changes in API*. To allow for the functioning of any applications using Data through the API, Contractor shall notify City in advance of any changes in the formatting of the API no later than thirty (30) days prior to the change.

12. DATA SECURITY.

a. Contractor shall at all times comply with the Contract Documents, Good Financial Industry and Accounting Practices, Applicable Laws, City's Red Flag Policy, SAS70 auditing standards, and the CITY's Cloud Computing Requirements.

b. Contractor shall comply with the City's Red Flag policy and timely report any Red Flags to the CITY's Program Administrator. Said report shall include Red Flags detected by Contractor or its subcontractors or subsidiaries and Contractor's response to the Red Flags so detected.

c. Contractor shall provide City with a copy of its existing Red Flag policies and procedures, and shall promptly provide copies of any changes to its Red Flag policies and procedures.

d. If any Software upgrade includes the storage or use of credit cards and debit cards, Contractor shall comply and shall warrant that the Contractor's software and services comply with the Payment Card Industry (PCI) Data Security Standards; Good Financial Industry and Accounting Practices; SAS70 auditing standards; Visa, Mastercard, and Discover Card Rules and Regulations; NACHA (The Electronic Payments Association) Rules; and the City's Red Flag Policy.

e. *Duty to Report*. Contractor shall maintain the security of City content and data and that of City's customers and any user that is stored in or in any way connected with Software Products and applications. If either Party believes or suspects that security has been breached or data compromised whether it be from harmful code or otherwise, the Party shall notify the Other Party of the issue or possible security breach within forty-eight (48) hours.

f. *Binding Subcontractors and Subsidiaries to Data Security Standards.* Contractor shall include similar provisions in Contractor's Agreements with subcontractors and subsidiaries who perform work or services related to these Software Products and or the City's Data contained therein or in the cloud storage.

13. NO HARMFUL CODE. Contractor warrants that the Software Products do not contain Harmful Code. For purposes of this Agreement, "Harmful Code" is any code

containing any program, routine, or device which is designed to delete, disable, deactivate, interfere with or otherwise harm any software, program, data, device, system or service, including without limitation, any time bomb, virus, drop dead device, malicious logic, worm, Trojan horse or trap or back door. Contractor shall include in contracts with any subcontractor a provision which prohibits the use of Harmful Code.

14. CONTRACTOR'S INSURANCE. The CONTRACTOR shall not commence work under this Contract until they have obtained all insurance required under this paragraph and such insurance has been approved by the CITY, nor shall the CONTRACTOR allow any subcontractor to commence work on the Project until all similar insurance required of subcontractor has been so obtained and approved. All policies shall be in amounts, form, and with companies satisfactory to the CITY which must carry an A-6 or better rating as listed in the A.M. Best or equivalent rating guide.

a. WORKERS COMPENSATION INSURANCE: The CONTRACTOR shall take out and maintain during the life of this Contract Employers Liability and Workers Compensation Insurance for all of their employees employed at the site of the work, and in case any work is sublet, the CONTRACTOR shall require the subcontractor similarly to provide Workers Compensation Insurance for all of the latter's employees unless such employees are covered by the protection afforded by the CONTRACTOR. Workers Compensation coverage shall meet Missouri statutory limits. Employers Liability limits shall be $500,000.00 each employee, $500,000.00 each accident, and $500,000.00 policy limit. Jn case any class of employees engaged in hazardous work under this Contract at the site of the work is not protected under the Workers Compensation Statute, the CONTRACTOR shall provide and shall cause each subcontractor to provide Employers Liability Insurance for the protection of their employees not otherwise protected.

b. COMMERCIAL GENERAL LIABILITY INSURANCE: CONTRACTOR shall carry Commercial General Liability Insurance written on ISO occurrence form CG 00 01 07 98 or later edition (or a substitute form providing equivalent coverage) and shall cover all operations by or on behalf of the CONTRACTOR, providing insurance for bodily injury liability and property damage liability for the limits indicated below and for the following coverage:

(1) Premises and Operations
(2) Products and Completed Operations

Contractual Liability insurance for the obligations assumed by the CONTRACTOR under this Contract.

Personal Injury Liability and Advertising Injury Liability.

Except with respect to bodily injury and property damage included within the products and completed operations hazards, the general aggregate limit shall apply separately to the CONTRACTOR's Project under this Contract. Completed Operations coverage must be maintained for the correction period provided by the Agreement.

Limit of Liability. The Commercial General Liability policy limits shall not be less than:

$1 Each Occurrence (Combined Single Limit for Bodily Injury and Property Damage)

$1 Aggregate for Products/Completed Operations

$1 Personal Injury/Advertising Injury

$1 General Aggregate (provide endorsement to apply the General Aggregate per project, if available. If not, see Umbrella Liability section.)

Additional Insured. CITY, all of its officers, directors and employees, shall be named as Additional Insureds under the Commercial General Liability Insurance using ISO Additional Insured Endorsements CG 20 10 or substitute providing equivalent coverage. If additional insured status is required for a correction period then CG 20 37 or equivalent should also be used. These endorsements must be stated on the insurance certificate provided to CITY and a copy of the endorsements confirming coverage should accompany the insurance certificate.

Primary Coverage. The CONTRACTOR's Commercial General Liability Policy shall apply as primary insurance and any other insurance carried by CITY shall be excess only and will not contribute with CONTRACTOR's insurance. This must be stated on the insurance certificate and a copy of the endorsement confirming coverage should accompany the insurance certificate.

c. BUSINESS AUTOMOBILE LIABILITY INSURANCE: The policy should be written on ISO form CA 0001 , CA 0005, CA 0002, CA0020 or a substitute form providing equivalent coverage and shall provide coverage for all owned, hired and non-owned vehicles. The limit of liability should be at least $1 Combined Single Limit for Bodily Injury and Property Damage each accident and should also cover Automobile Contractual Liability. The policy should name CITY and all of its officers, directors and employees as Additional Insureds. The policy shall be endorsed to be primary coverage and any other insurance carried by CITY shall be excess only and will not contribute with CONTRACTOR's insurance. To confirm coverage, a copy of the Additional Insured Endorsement should accompany the insurance certificate.

d. UMBRELLA EXCESS LIABILITY: The CONTRACTOR should provide an umbrella excess liability policy that will provide a minimum of $1 per occurrence/$l ,000,000 aggregate over the above listed coverages. This policy should "follow-form" of the underlying policies and complies with all insurance requirements of those policies. If the General Aggregate of the Commercial General Liability policy does not apply per project, the umbrella excess limits should be $2,000,000 per occurrence/$2,000,000 aggregate.

e. WAIVER OF SUBROGATION: The Commercial General Liability and Automobile Liability policies shall each contain a waiver of subrogation in favor of CITY and its officers, directors and employees.

f. CERTIFICATES OF INSURANCE: As evidence of the insurance, limits and endorsements required, a standard ACORD or equivalent Certificate of Insurance executed by a duly authorized representative of each insurer shall be furnished by the CONTRACTOR to the CITY before any work on this Project is commenced by the CONTRACTOR. CITY shall have the right, but not the obligation, to prohibit CONTRACTOR or any Subcontractor from entering the Project site until such certificates are received and approved by the CITY. With respect to insurance to be maintained after final payment, an additional certificate(s) evidencing such coverage shall be promptly provided to CITY as a precondition to final payment. The Certificate of Insurance shall provide that there will be no cancellation or reduction of coverage without thirty (30) days prior written notice to CITY. The certificate must also contain a description of the Project. Failure to maintain the insurance required herein may result in termination of the Contract at CITY's option. In the event the CONTRACTOR does not comply with the requirements of this section, CITY shall have the right, but not the obligation, to provide insurance coverage to protect CITY and charge the CONTRACTOR for the cost of that insurance. The required insurance shall be subject to the approval of CITY, but any acceptance of insurance certificates by CITY shall in no way limit or relieve the CONTRACTOR of their duties and responsibilities in this Agreement.

g. SUBCONTRACTORS: CONTRACTOR shall cause each Subcontractor to purchase and maintain insurance of the types and amounts specified herein. Limits of such coverage may be reduced only upon written agreement of CITY. CONTRACTOR shall provide to CITY copies of certificates evidencing coverage for each Subcontractor. Subcontractors' commercial general liability and business automobile liability insurance shall name CITY as Additional Insured and have the Waiver of Subrogation endorsements added.

15. HOLD HARMLESS AGREEMENT. To the fullest extent not prohibited by law, Contractor shall indemnify and hold harmless the City of Columbia, its directors, officers, agents, and employees from and against all claims, damages, losses, and expenses (including but not limited to attorney's fees), of any subcontractor (meaning anyone, including but not limited to consultants having a contract with Contractor or a subcontractor for part of the services), of anyone directly or indirectly employed by Contractor or by any subcontractor, or of anyone for whose acts the Contractor or its subcontractor may be liable, in connection with providing these services. This provision does not, however, require Contractor to indemnify, hold harmless, or defend the CITY from its own negligence. Nothing in this Agreement shall constitute a waiver of sovereign immunity.

16. NOTICE. Each notice, request, demand, statement or routine communication required or permitted under this Agreement, or any notice or communication that either Party may desire to deliver to the other, shall be in writing and shall be considered delivered effective: (a) when verified by written receipt if sent by personal courier, overnight courier, or mail; or (b) when verified by automated receipt or electronic logs if sent by facsimile or email.

The designation and titles of the person to be notified or the address of such person may be changed at any time by written notice.

IF TO CITY:

City of Columbia, MO
Finance Department
ATTN: Purchasing Agent
P.O. Box 6015
Columbia, MO 65205

IF TO CONTRACTOR:

ETA Transit Systems
Attn: Nicole Castonguay- CEO
6420 Congress AVE STE 1850
Boca Raton FL 33487

With a copy to:

City of Columbia, MO
Public Works Department
ATTN: Transit Manager
P.O. Box 6015
Columbia, MO 65205

17. AMENDMENT. No amendment, addition to, or modification of any provision hereof shall be binding upon the Parties, and neither Party shall be deemed to have waived any provision or any remedy available to it unless such amendment, addition, modification or waiver is in writing and signed by a duly authorized officer or representative of the Parties.

18. ASSIGNMENT. This Agreement shall inure to the benefit of and be binding upon the Parties and their respective successors and permitted assigns. Neither Party shall assign this Agreement or any of its rights or obligations hereunder without the prior written consent of the other Party.

19. SEVERABILITY. If any of the terms of this Agreement are finally held or determined to be invalid, illegal or void, all other terms of the Agreement shall remain in effect; provided that the Parties shall enter into negotiations concerning the terms affected by such decision for the purpose of achieving conformity with requirements of any applicable law and the intent of the Parties.

20. NO THIRD PARTY BENEFICIARY. This Agreement is intended solely for the benefit of the Parties hereto and nothing contained herein shall be construed to create any duty to, or standard of care with reference to, or any liability to, or any benefit for, any Person not a Party to this Agreement.

21. GOVERNING LAW. This Agreement shall be governed by, interpreted and enforced in accordance with the laws of the State of Missouri and/or the laws of the United States, as applicable. The venue for all litigation arising out of, or relating to this Agreement, shall be Boone County, Missouri, or the United States Western District of Missouri. The Parties hereto irrevocably agree to submit to the exclusive jurisdiction of such courts in the State of Missouri and waive any defense of forum non conveniens.

22. NATURE OF CITY'S OBLIGATIONS. All obligations of the City under this Agreement, which require the expenditure of funds, are conditional upon the availability of funds budgeted and appropriated for that purpose.

23. GENERAL LAWS. Contractor agrees to comply with all applicable laws, rules, regulations, ordinances, and statutes of the United States, State of Missouri, and City of Columbia, Missouri.

24. EMPLOYMENT OF UNAUTHORIZED ALIENS PROHIBITED. Contractor agrees to comply with Missouri State Statute section 285.530 in that they shall not knowingly employ, hire for employment, or continue to employ an unauthorized alien to perform work within the state of Missouri. As a condition for the award of this contract the Contractor shall, by sworn affidavit and provision of documentation, affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services. Contractor shall also sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. Contractor shall require each subcontractor to affirmatively state in its contract with Contractor that the subcontractor shall not knowingly employ, hire for employment or continue to employ an unauthorized alien to perform work within the state of Missouri. Contractor shall also require each subcontractor to provide Contractor with a sworn affidavit under the penalty of perjury attesting to the fact that the subcontractor's employees are lawfully present in the United States.

25. AMERICANS WITH DISABILITIES ACT. Contractor's Software Products and applications shall comply with the requirements of the Americans with Disabilities Act and comply with the requirements of any rules or regulations of the federal, state, or local government related thereto.

26. COMPLIANCE WITH GRANT REQUIREMENTS. The Parties agree that grant funds from the United States Department of Transportation (hereinafter, "FTA") are being used for this purchase. Contractor shall comply with all conditions and requirements of the Grant, including, but not limited to those set forth herein. Contractor shall include in contracts with subcontractors provisions that require subcontractors to comply with the requirements of this section.

a. 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 Agreement between the City and FTA (FTA MA (18) dated October 1 , 2011), 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.

b. CIVIL RIGHTS.

1. Nondiscrimination. In accordance with Title VI of the Civil Rights Act, as amended, 42 U.S.C. § 2000d, section 303 of the Age Discrimination Act of

1 975, as amended, 42 U.S.C. § 6102, section 202 of the Americans with Disabilities Act of 1990, 42 U.S. C. § 12132, and 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, creed, national origin, sex, age, or disability. In addition, the Contractor agrees to comply with applicable Federal implementing regulations and other implementing regulations that the Federal Transit Administration (FTA) may issue.

2. Equal Employment Opportunity. The following equal employment opportunity requirements apply to this Contract: Race, Color, Creed, National Origin or Sex. In accordance with Title Vll 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 opportunity requirements of the 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. Parts 60 et seq., (which implement Executive Order No. 1 1246, "Equal Employment Opportunity," as amended by Executive Order No. 1 1375, "Amending Executive Order 1 1246 Relating to Equal Employment Opportunity," 42 U.S.C. 2000e note), and with any applicable Federal statutes, executive orders, regulations, and Federal policies that may in the future affect activities undertaken in the course of the Project. 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, creed, national origin, sex, or age. 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. In addition, the Contractor agrees to comply with any implementing requirements FTA may issue.

Age. In accordance with Section 4 of the Age Discrimination in Employment Act of 1967, as amended, 29 U.S.C. § 623 and Federal transit law at 49 U.S.C. §5332, the Contractor agrees to refrain from discrimination against present and prospective employees for reason of age. In addition, the Contractor agrees to comply with any implementing requirements FTA may issue.

Disabilities. In accordance with section 102 of the Americans with Disabilities Act, as amended, 42 U.S.C. §121 12, the Contractor agrees that it will comply with the requirements of U.S. Equal Employment Opportunity Commission, "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 C.F.R. Part 1630, pertaining to employment of persons with disabilities. In addition, the Contractor agrees to comply with any implementing requirements FTA may issue.

ADA Access Requirements. In accordance with section 102 of the Americans with Disabilities Act, as amended, 42 U.S.C. § 121 12 and section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794, the Contractor agrees that it will comply with the requirements of U.S. Department of Transportation

regulations, "Transportation Services for Individuals with Disabilities (ADA)," 49 CFR Part 37; and U.S. Department of Transportation regulations, "Americans with Disabilities Accessibility Specifications for Transportation Vehicles," 36 CFR Part 1192 and 49 CFR Part 38, pertaining to facilities and equipment to be used in public transportation. In addition, the Contractor agrees to comply with the requirements of 49 U.S.C. S 5301 (d) which expresses the Federal policy that the elderly and persons with disabilities have the same right as other persons to use mass transportation services and facilities, and that special efforts shall be made in planning and designing those services and facilities to implement transportation accessibility rights for elderly persons and persons with disabilities. CONTRACTOR shall make the services, programs, and activities governed by this Agreement accessible to the disabled as required by the Americans with Disabilities Act and its implementing regulations.

c. DEBARMENT AND SUSPENSION CERTIFICATION. The Contractor, its principals and any affiliates, shall certify that it is not included in the "U.S. General Services Administration's List of Parties Excluded from Federal Procurement or Non-procurement Programs," as defined at 49 CFR Part 29, Subpart C. The Contractor agrees to refrain from awarding any subcontract of any amount (at any tier) to a debarred or suspended subcontractor, and to obtain a similar certification from any subcontractor (at any tier) seeking a contract exceeding $25,000. The Contractor agrees to provide the City a copy of each conditioned debarment or suspension certification provided by a prospective subcontractor at any tier, and to refrain from awarding a subcontract with any party that has submitted a conditioned debarment or suspension certification until FTA approval is obtained. Contractor also agrees to comply with any implementing requirements FTA may issue.

d. DISADVANTAGED BUSINESS ENTERPRISE (DBE). This Contract is subject to the requirements of Title 49, Code of Federal Regulations, Part 26, Participation by Disadvantaged Business Enterprises in Department of Transportation Financial Assistance Programs. The national goal for participation of Disadvantaged Business Enterprises (DBE's) is 10 percent. The City's overall goal for DBE participation is 12.5 percent. A separate contract goal has not been established for this procurement. CONTRACTOR 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 CFR Part 26 in the award and administration of this DOT-assisted contract. 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 City deems appropriate. Each subcontract the CONTRACTOR signs with a subcontractor must include the assurance in this paragraph (see 49 C.F.R. 26.13(b)). CONTRACTOR shall be required to report its DBE participation obtained through race-neutral means throughout the Term. 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 from CITY. CONTRACTOR must promptly notify CITY 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. CONTRACTOR may not terminate any DBE subcontractor and perform that work through its own forces or those of an affiliate without the prior written consent of CITY.

e. DISCLAIMER OF FEDERAL GOVERNMENT OBLIGATIONS OR LIABILITY. CONTRACTOR, and any subcontractors acknowledge and agree that, notwithstanding any concurrence by the Federal Government in or approval of the solicitation or award of this 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 CONTRACTOR, or any other party (whether or not a party to this Contract) pertaining to any matter resulting from this Contract. It is further agreed that the clause shall be included in each subcontract and shall not be modified, except to identify the subcontractor who will be subject to its provision.

f. ENVIRONMENTAL REGULATIONS.

1. Clean Air. 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. CONTRACTOR agrees to report, and to require each subcontractor at every tier receiving more than $100,000 from this Contract to report any violation of these requirements resulting from any project implementation activity to CITY. CITY will in turn, report each violation as required to assure notification to FTA and the appropriate U.S. EPA Regional Office.

2. Clean Water. 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. CONTRACTOR agrees to report, and requires each subcontractor at every tier receiving more than $100,000 from this Contract to report any violation of these requirements resulting from any project implementation activity to the CITY. CONTRACTOR understands that the CITY will in turn, report each violation as required to assure notification to FTA and the appropriate U.S. EPA Regional Office.

3. Energy Conservation. 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.

4. Recovered Materials/Recycle Products. CONTRACTOR agrees to comply with all the requirements of Section 60002 of the Resource Conservation and Recovery Act (RCRA), as amended (42 U.S.C. 6962), including but not limited to the regulatory provisions of 40 CFR Part 247, and Executive Order 12873, as they apply to the procurement of the items designated in Subpart B of 40 CFR Part 247.

g. FRAUD AND FALSE OR FRAUDULENT STATEMENTS OR RELATED ACTS. CONTRACTOR acknowledges that the provisions of the Program Fraud Civil Remedies Act of 1986, as amended, 31 U.S.C. § 3801 et seq. and U.S DOT regulations, "Program Fraud Civil Remedies," 49 CFR Part 31 , apply to its actions pertaining to the Project. Upon execution of the Contract, CONTRACTOR certifies and affirms the truthfulness and accuracy of any statement it has made, it makes, or may make pertaining to the project covered under this Contract. In addition to other penalties that may be applicable, CONTRACTOR further acknowledges that if it makes a false, fictitious, or fraudulent claim, statement, submission, or certification, the Federal Government reserves the right to impose the penalties of the Program Fraud Civil Remedies Act of 1986 on CONTRACTOR to the extent the Federal Government deems appropriate. CONTRACTOR also acknowledges that if it makes, or causes to be made, a false, fictitious, or fraudulent claim, statement, submission, or certification to the Federal Government in connection with this Contract, the Government reserves the right to impose on the Contractor the penalties of 18 U.S.C. § 1001 and 49 U.S.C. § 53070) (1), to the extent the Federal Government deems appropriate. CONTRACTOR agrees to include these clauses in each subcontract, and it is further agreed that the clauses shall not be modified, except to identify the subcontractor who will be subject to the provisions.

h. INCORPORATION OF FEDERAL TRANSIT ADMINISTRATION TERMS. The provisions in this Contract include certain standard terms and conditions required by the U.S. Department of Transportation (DOT), whether or not expressly set forth. All contractual provisions required by DOT, as set forth in FTA Circular 4220. IE or any revision thereto, are hereby incorporated by reference. Anything to the contrary herein notwithstanding and to the extent allowed by law, all FTA mandated terms shall be deemed to control in the event of a conflict with other provisions contained in the Contract. CONTRACTOR shall not perform any act, fail to perform any act, or refuse to comply with any the CITY requests that would cause the CITY to be in violation of the FTA terms and conditions.

i. LOBBYING RESTRICTIONS. CONTRACTOR is bound by its certification contained in its offer to the CITY regarding the use of federal or non-federal funds to influence, or attempt to influence any federal officer or employee regarding the award, execution, continuation, or any similar action of any federal grant or other activities as defined in 31 U.S.C. 1352, and 49 CFR Part 20. CONTRACTOR agrees to comply with this requirement throughout the term of the Contract. CONTRACTOR shall obtain the same certification and disclosure required by the LOBBYING RESTRICTIONS from each subcontractor and shall file the required certifications and disclosures with the CITY.

j. NATIONAL INTELLIGENT TRANSPORTATION SYSTEMS ARCHITECTURE AND STANDARDS. CONTRACTOR agrees to conform, to the extent applicable, to the National Intelligent Transportation Systems (ITS) Architecture and Standards as required by SAFETEA-LU § 5307(c), 23 U.S.C. § 512 note, and CONTRACTOR agrees to comply with FTA Notice, "FTA National ITS Architecture

Policy on Transit Projects" 66 Fed. Reg. 1455, January 8, 2001, and any further implementing directives, except to the extent FTA determines otherwise in writing.

k. PRIVACY ACT REQUIREMENTS. CONTRACTOR agrees to comply with, and assures the compliance of its employees and subcontractors with the information restrictions and other applicable requirements of the Privacy Act of 1 974, 5 U.S.C. S 552. Among other things, CONTRACTOR agrees to obtain the express consent of the CITY and/or the Federal Government before the CONTRACTOR or its employees operate a system of records on behalf of the CITY or Federal Government. CONTRACTOR understands that the requirements of the Privacy Act, including the civil and criminal penalties for violation of that Act, apply to all individuals involved, and that failure to comply with the terms of the Privacy Act may result in termination of the underlying Agreement. CONTRACTOR agrees that strict privacy will be maintained in the collection, storage, use, transfer, access to and/or security of information protected by the Privacy Act. CONTRACTOR agrees to protect such information, and to limit the use of the information to that required by the contract.

l. RECORD RETENTION AND ACCESS. CONTRACTOR agrees that, during the course of this Agreement and any extensions thereof, and for three years thereafter, it will maintain intact and readily accessible all data, documents, reports, records, contracts, and supporting materials relating to this Contract. In the event of litigation or settlement of claims arising from the performance of this Contract, CONTRACT shall maintain same until such litigation, appeals, claims or exceptions related thereto have been disposed of. CONTRACTOR shall permit the CITY, the Secretary of Transportation, the FTA Administrator, the Comptroller General of the United States, and, the CITY to inspect all work, materials, sites, payrolls, and other data and records, and to audit the books, records, and accounts of CONTRACTOR relating to its performance under this Contract. CONTRACTOR shall permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

m. SEAT BELT USE POLICY. CONTRACTOR agrees to comply with terms of Executive Order No. 13043 "Increasing Seat Belt Use in the United States."

n. TEXTING WHILE DRIVING AND DISTRACTED DRIVING. Consistent with Executive Order No. 13513, "Federal Leadership on Reducing Text Messaging While Driving," October 1 , 2009, 23 U.S.C. Section 402 note, and DOT Order 3902.10, "Text Messaging While Driving," December 30, 2009, CONTRACTOR agrees to promote policies and initiatives for its employees and other personnel that adopt and promote safety policies to decrease crashes by distracted drivers, including policies to ban text messaging while driving, and to encourage each subcontractor to do the same.

o. BUY AMERICA. CONTRACTOR shall comply with 49 U.S.C. S5323(j), and 49 CFR. Part 661 , which provide that federal funds may not be obligated unless steel, iron, and manufactured products used in FTA-funded projects are produced in the United States, unless a waiver has been granted by FTA or the product is subject to a general waiver. General waivers are listed in 49 CFR 661 .7 and include final assembly in

the United States for 15 passenger vans and 15 passenger wagons produced by Chrysler Corporation, microcomputer equipment & software. Separate requirements for rolling stock are set out at 53230) (2) (C) and 49 CFR Part 661.11 . Rolling stock not subject to a general waiver must be manufactured in the United States and have a 60 percent domestic content.

27. CONTRACTOR'S REPRESENTATIONS AND WARRANTIES. CONTRACTOR represents and warrants as follows:

a. Contractor is a corporation with authority to transact business in the State of Missouri;

b. Contractor has the power and authority to enter into and perform this Agreement and is not prohibited from entering into this Agreement or discharging and performing all covenants and obligations on its part to be performed under and pursuant to this Agreement;

c. Contractor has taken all action required by law in order to approve, execute and deliver this Agreement;

d. The execution and delivery of this Agreement, the consummation of the transactions contemplated herein and the fulfillment of and compliance by Contractor with the provisions of this Agreement will not conflict with or constitute a breach of or a default under or require any consent, license or approval that has not been obtained pursuant to any of the terms, conditions or provisions of any law, rule or regulation, any order, judgment, writ, injunction, decree, determination, award or other instrument or legal requirement of any court or other agency of government, the documents of formation of Contractor or any contractual limitation, restriction or outstanding trust indenture, deed of trust, mortgage, loan agreement, lease, other evidence of indebtedness or any other agreement or instrument to which CONTRACTOR is a party or by which it or any of its property is bound and will not result in a breach of or a default under any of the foregoing;

e. Contractor has taken all such action as may be necessary or advisable and proper to authorize this Agreement, the execution and delivery hereof, and the consummation of transactions contemplated hereby;

f. To Contractor's knowledge, there are no actions, proceedings, judgments, rulings or orders issued by, or pending before any court or other governmental body that would materially adversely affect Contractor's ability to perform its obligations under this Agreement; and

g. This Agreement is a legal, valid and binding obligation of CONTRACTOR enforceable in accordance with its terms, except as limited by laws of general applicability limiting the enforcement of creditor's rights or by the exercise of judicial discretion in accordance with general principles of equity.

28. USE OF SUBCONTRACTORS. The Parties agree that Contractor shall subcontract using the subcontractors Contractor identified in Exhibit A. No additional or other substitute subcontractor shall be used without the prior written approval of the City. Contractor shall file with City a complete list of subcontractors together with a list of the services and equipment provided by subcontractor. This list shall be submitted in writing to the City as soon as subcontracts are made and approved by the City. Any subcontractor performing work under this contract at the direction of the Contractor shall file a "Final Receipt of Payment and Release" form. This completed form shall be submitted to the CITY along with application for final payment.

29. NO WAIVER OF IMMUNITIES. In no event shall the language of this Agreement constitute or be construed as a waiver or limitation for either Party's rights or defense with regard to each Party's applicable sovereign, governmental, or official immunities and protections as provided by federal and state constitution and laws.

30. MISSOURI ANTI-DISCRIMINATION AGAINST ISRAEL ACT. Pursuant to Missouri Revised Statute Section 34.600, Contractor certifies it is not currently engaged in and shall not, for the duration of this Agreement, engage in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel.

31. GENERAL NONDISCRIMINATION. Pursuant to Chapter 12 of the Code of Ordinances of the City of Columbia, Missouri, Contractor, and any subcontractor thereof, agrees to comply with all state, federal and local regulations regarding unlawful discrimination.

32. ELECTRONIC AGREEMENT AND COUNTERPARTS. This Agreement may be signed in one or more counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same document. Faxed signatures, or scanned and electronically transmitted signatures, on this Agreement or any notice delivered pursuant to this Agreement, shall be deemed to have the same legal effect as original signatures on this Agreement.

33. ENTIRE AGREEMENT. This Agreement represents the entire and integrated agreement between the Parties relative to the contracted services herein. All previous or contemporaneous contracts, representations, promises and conditions relating to the contracted services herein are superseded.

[SIGNATURES ON FOLLOWING PAGE]

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized representatives as of the date of the last signatory to this Agreement.

CITY OF COLUMBIA, MISSOURI

BY: _____ SSC
De'Carlon Seewood, City Manager

DATE: _____

ATTEST:

By: _____
Sheela Amin, City Clerk

APPROVED AS TO FORM:

By: _____
Nancy Thompson, City Counselor / AK

CERTIFICATION: I hereby certify that this Agreement is within the purpose of the appropriation to which it is to be charged, account(s) to be determined at the time of the purchase order, and that there is an unencumbered balance to the credit of such account(s) sufficient to pay therefore.

BY: _____
Matthew Lue, Director of Finance

ETA PHI SYSTEMS, INC.

BY: Nicole Castonguay

PRINTED NAME: Nicole Castonguay

TITLE: CEO

DATE: 6/7/2024

ATTEST:

BY: _____

TITLE: _____

EXHIBIT A

CONTRACTOR'S RESPONSE TO CITY RFP 128/2023

128/2023 Addendum 4
ETA Transit Systems
ETA Phi Systems, Inc
Supplier Response

Event Information

Number:	128/2023 Addendum 4
Title:	Intelligent Transportation Systems (ITS) Services
Type:	Request for Proposal
Issue Date:	6/26/2023
Deadline:	8/11/2023 05:00 PM (CT)
Notes:	Proposals may be submitted in a sealed envelope at the Purchasing Division office or uploaded electronically on this e-bidding website. Sealed proposals must be delivered to the Purchasing Division, 701 E. Broadway, 5th Floor, Columbia, MO 65201 by the closing date and time. Proposals received after the appointed time will be time stamped and marked as late. Late proposals will not be opened and will not be considered in the evaluation. Proposals must be in a sealed envelope and marked in bold letters “RFP 128/2023”. No fax or e-mail proposals shall be accepted.

ETA Transit Systems Information

Contact: sales
Address: 7700 Congress Ave
STE 2201
Boca Raton, FL 33487
Phone: (800) 382-0917
Email: sales@etatransit.com
Web Address: www.etatransit.com

By submitting your response, you certify that you are authorized to represent and bind your company.

Jariel Adler
Signature

jadler@etatransit.com
Email

Submitted at 8/11/2023 01:22:58 PM (CT)

Supplier Note

Thank you for the opportunity to present our proposal. We will also be submitting a proposal for 130/2023 - APCs.

Response Attachments

ETA Proposal for RFP 1282023 – Intelligent Transportation System (ITS) Services .pdf

ETA Transit's proposal for RFP 128/2023 - ITS

GoCOMO

RFP#: 128/2023 – Intelligent Transportation Systems (ITS) Services

etatransit.com

Title: Transit ITS Procurement
Due: August 11, 2023
Submitted by:

ETA Transit Systems, Inc.
7700 Congress Avenue, Suite 2201
Boca Raton, FL 33487

What drives you?

Table of Contents

Confidential Information

Sections bearing a lock icon are to be treated as confidential or trade secret information. This information may not be made public or shared with anyone outside the decision-making committee for this procurement effort. Unless expressly noted, all images and content contained under a confidential header are considered protected information.

To the members of the GoCOMO team,

ETA Transit Systems (ETA) recognizes the energy that the City of Columbia has put forth in providing the community with safe, reliable, and courteous service. As stated in the City of Columbia's 2050 Long-Range Transportation Plan (LRTP), a key focus is on enhancing services to meet residents' needs. Among the identified objectives, ETA & the SPOT™ system can play a pivotal role in achieving Goal 2, Objective 3, which aims to reduce dependence on automobile travel and better cater to non-vehicle owners and drivers. By leveraging ETA's traveler information systems, GoCOMO will bolster ridership by providing your passengers tools, such as ETA's mobile app and trip planner, which deliver real time information that will continue to build confidence in Columbia's transportation network.

With over 100 projects deployed in the past 20 years, ETA has the right mix of people, skills, and experience to ensure your success. We believe that there are four pillars to a successful CAD/AVL project – Industry experience, Engineering, Software, Project Management approach, and customer service.

Experience: You can take comfort knowing that ETA has delivered identical systems for many other cities and universities. In fact, ETA installed Valley Regional Transit's hardware on its fleet of 67 vehicles in less than five weeks in 2021. Or more recently (July) at AppalCART/Appalachian State University – Boone, NC, ETA successfully deployed their entire 29 bus system in under 4 weeks. **ETA will complete GoCOMO's installation of equipment on all 25 buses within eight weeks of a purchase order.**

Hardware Engineering: Failed CAD/AVL projects are typically due to unreliable onboard equipment that ultimately leads to poor customer service. The City of Columbia requires a reliable system from a reputable provider to disseminate real-time information to riders and to power transit operations. While other vendors could satisfy your core software requirements, there are very few that can support the advanced integration requirements on a properly designed onboard equipment platform. Many vendors will offer tablets or all-in-one computers; these are simply not rugged enough for GoCOMO's environment. ETA is different. In addition to meeting GoCOMO's software requirements, our system is installed on transit-grade equipment that has been in revenue service for over two decades. Our properly engineered system will ensure reliability to the City of Columbia and its community of riders.

Cloud-based software: The SPOT™ software operates entirely in the cloud and is finely tuned for Chrome, while remaining compatible with all major web browsers. This approach alleviates the operational demands on GoCOMO's IT department by eliminating the need to oversee an additional system In

addition, our industry leading Route Manager module ensures that GoCOMO can manage detours, schedules, and their GTFS real time. **GoCOMO can adapt to critical circumstances without waiting on the vendor.** The ETA system meets 100% of the City of Columbia's immediate needs with unmatched expansion capabilities to support your future growth.

Project management: A thriving technology project also relies on a clear and effectively executed implementation plan. Key elements for success encompass early and regular communication, a sound engineering design, comprehensive training, and extensive testing. Joshua Adler, your devoted project manager, employs a refined implementation approach developed over numerous years. This method guarantees that GoCOMO's data is optimized, system is thoroughly tested, and all users are properly trained prior to launch.

Support: Finally, GoCOMO deserves a partner with a lasting commitment to customer service. Since 2003, ETA has deployed over 100 projects nearly identical in size and scope. Dozens of transit agencies have benefited from ETA's free refresher training, custom reports, software updates, and team of expert customer service professionals. We invite you to contact the Valley Regional Transit, Toledo Area Regional Transit Authority, and AppalCART as references to learn more about their experiences with our services.

ETA has earned a reputation for providing exceptional service. Since 2020 ETA has witnessed a remarkable growth in customer loyalty, as demonstrated by the renewal status of our projects. **Out of the twenty-six customer projects that were up for renewal during this period, an overwhelming twenty-five clients have chosen to continue their partnerships with ETA.** This impressive retention rate is largely attributed to the consistently exceptional support provided by our customer service team. The City of Columbia will receive the same outstanding service for the duration of our partnership.

Thank you for considering ETA Transit System's proposal. Once again, we appreciate the opportunity to present our proposal and look forward to the possibility of working together.

Warm regards,

Nicole Castonguay

Nicole Castonguay, CEO
ncastonguay@etatransit.com

Executive summary

At ETA, we are acutely aware of the mounting pressures that GoCOMO and the industry as a whole face in order to satisfy the needs of all stakeholders. We recognize that:

- The burden of unfunded mandates, such as safety and environmental regulations, puts additional stress on already constrained resources.
- The challenges posed by rising labor costs and employee turnover which disrupt operations and hinder productivity.
- The time-consuming nature of board presentations, taking focus away from other crucial tasks.
- The complexity and demands of NTD (National Transit Database) reporting requirements.

You are stretched thin, and you need technology to make life easier. A system that streamlines tasks, reducing the time and effort spent on mundane, repetitive duties.

Our proposal will showcase why we are the ideal partner to address the City of Columbia's pressing concerns and establish a lasting partnership spanning a decade or more. ETA differentiates itself in the following ways:

Engineering know-how

ETA's staff includes a team of industry veterans specializing in electrical and mechanical engineering. This expertise is essential to deliver onboard systems that meet the stringent requirements of GoCOMO. Unlike "software only" suppliers, ETA understands the importance of combining hardware and software solutions to enable GoCOMO to acquire real-time data from their buses. This data is crucial for monitoring and managing the fleet effectively, NTD reporting, and passenger information.

Industry experience

ETA started providing CAD/AVL systems prior to the existence of cellular networks! Our dedicated team has successfully deployed more than 100 systems comparable in scale to those required by GoCOMO, along with numerous high-value projects surpassing $10 million each. With our wealth of expertise, we guarantee the flawless delivery of GoCOMO's system from the very first attempt.

Software capabilities

ETA's software platform goes beyond fulfilling your essential needs. It equips you with a range of tools to identify and address inefficiencies in your service delivery, streamline NTD reporting through automation, rapidly generate detours and convey service disruptions, and notifies GoCOMO of anomalies and exceptions. ETA upgrades its system every two (2) weeks (no kidding) so that the City of Columbia benefits from enhancements, new features, and custom reports.

GoCOMO will leverage ETA's leading CAD/AVL solution to:

- Improve on-time performance
- Increase bus operator safety
- Automate NTD reporting
- Foster communication between GoCOMO staff and riders
- Improve customer satisfaction
- Expedite adjustments to service interruptions

ETA has earned a reputation as a dependable CAD/AVL provider. In the past 3 years, an impressive 96% of our customers have chosen to continue their partnership with ETA. Given our considerable experience and high customer retention rate, the City of Columbia can trust that ETA will deliver on our promises. Together, we will work towards enhancing operating efficiencies and elevating the passenger experience.

SATISFACTION	MARKET PENETRATION	PROJECT MANAGEMENT
96% of ETA customers have renewed their service since 2020.	Over the last 10 years, ETA Transit has grown 5X	12 weeks is the average length of project deployment time.

STABILITY	LONGEVITY	EXPERIENCE
Revenue growth since 2020: 2X	21 years in business	Average years of transit experience of ETA staff 9

ETA's proposal is compliant with GoCOMO's RFP and includes:

Items required by RFP	
▪ On-board equipment ▪ Automatic Vehicle Location ▪ Interior message signs ▪ Dispatch software ▪ Reports ▪ GTFS/GTFS-RT ▪ APC integration ▪ Operator software	▪ Information systems ▪ Mobile app and web app ▪ Automatic on-board announcements ▪ MDT single-sign on ▪ Optional signage for bus stops ▪ Service interruption and detour management system (Route Manager)

ETA certifies to GoCOMO:

- Includes all costs required to design, configure, install, test, deploy, and support GoCOMO. There are no hidden charges
- Ensures that the project will be delivered within twelve (12) weeks of notice to proceed
- Will minimize downtime during system cut-over
- Makes it easy to transfer equipment to new buses or have it installed at the OEM factory
- The City of Columbia will have the option to iFrame the bus tracker site to embed in your website
- Natively supports GTFS/GTFS-RT integration to technology partners such for fare collection, fixed route scheduling software, microtransit/demand-response software, and data warehouse systems.
- That we will be the POC for the entire project taking responsibility for all integrations
- Repeat training for the duration of the project at no additional cost

Quick Reference Guide

Requirement	Pg #	Comments
GoCOMO required signature pages	1	
GoCOMO required exhibits & pricing page	198	
ETA pricing page	189	
Automated Voice Annunciation (AVA)		
System must be able to perform audible and visual announcements of bus stops inside the bus, as well as audible announcements outside of the bus by use of speaker system.	87	
System must be satisfactory to Americans with Disabilities Association.	87	
Announcements must be made at predetermined distances from the bus stops.	57	Route manager allows GoCOMO to manage triggers and boundaries
System must be customizable to GoCOMO's specifications.	87	SPOT™ has hundreds of settings to help GoCOMO tailor the system to its needs.
System shall have a procedure for making public service announcements, service alerts and/or advertisements which can be triggered at predetermined locations.	57	Route manager allows GoCOMO to manage triggers and boundaries
System must allow for the volume to be easily adjusted for each vehicle.	87	
System shall allow for announcements to be played through all speakers of the bus, including the driver speaker.	87	

Automatic Vehicle Location (AVL)		
System must have a status screen for dispatchers to be able to view routes and the status of the buses running.	62	
System must show a bus in service/ out of service.	62	
System must allow the dispatcher to log buses on/off jobs, if necessary.	62	
System must show real time location of all assets at all times.	62	
System shall be configurable for detours and route adjustments from staff.	57	
Application (App)		
System shall allow for service alerts and public service announcements.	76	
System shall offer an app for passenger convenience downloadable for Apple and Android.	33	
System shall, for passenger convenience, offer a method to integrate with the City's existing MyCoMo mobile app and/or offer a mobile app for Apple and Android devices.	27	
System shall give passengers arrival information in real time	36	
System shall offer trip planning capacity for users	62	With APC integration, capacity can be displayed on the traveler information systems and administrative console
System shall offer ability to send notification, service alerts and public service announcements to users. This should include the ability for push notifications.	76	Mobile app users have the option to select alerts and receive push notifications

Additional features		
System shall offer a method to display route and bus location information on the City of Columbia website (www.como.gov).	33	
System shall offer an API that allows the City of Columbia to programmatically request bus stop information (i.e. estimated time of arrival) in real time.	28	
The driver interface shall display time.	44	Driver OTP screen displays the time and route information
The driver interface must go to lockout screen and not be accessible while bus is in motion.	43	The MDT interface is locked while the vehicle is in motion. The system's "lock out" screen is configurable to display on-time performance, bus bunching status, or the system clock
Logon information shall list all available routes and if possible, notify when multiple logons to the same route occur.	46	
System must be able to have history of all buses available for review, showing timestamps and locations.	74	
System must allow for routes that span one day to the next (overnight).		The system natively supports this requirement
System must have reporting capabilities for federal reporting requirements, including but not limited to vehicle revenue miles and	65	

actual miles, schedule adherence, on-time performance, deadhead and service hours.		
System shall have ability to export all reports into formats such as excel and PDF.	65	
All equipment must be rugged enough to withstand harsh environments, temperature swings, vibration and jarring, humidity, etc.	40	
Contractor must provide training to all GoCOMO staff.	115	
Contractor must be willing to provide documentation of all systems for service and on-site troubleshooting. A maintenance plan must be included for preventative maintenance.	124	
Contractor must provide project management services to fully implement the system. This shall include timeline of implementation, procurement of equipment, installation, and any initial calibration and testing needed.	105	
Contractor shall provide ongoing maintenance and technical support for duration of the contract.	124	
Ongoing professional customer support shall be available via in-person, telephone, email or web for troubleshooting and service questions.	124	

GoCOMO required signature pages

[What you will discover]

This section outlines the City of Columbia's required addendum signature pages and RFP. These forms have been populated in order to ensure compliance per the RFP.

[Section key points]

- RFP Pg #1 – Signature page
- Addendum # 1 - Addition of exhibit H
- Addendum # 2 – Request for clarifications (re-issue)

Let's get started!

Transit agencies report that system performance, accurate transfer of route information, and training are the top three areas of concern when adopting a new CAD/AVL system.

— Source: 2020 ETA Transit Agency Survey

RFP Pg# 1 - Signature Page

This page was intentionally left blank.

SOLICITATION NO.: Request for Proposal (RFP) 128/2023
BUYER: Patrick Doll
PHONE NO.: (573) 874-7687
E-MAIL: Patrick.doll@como.gov

TITLE: Intelligent Transportation Systems (ITS) Services

ISSUE DATE: June 26th, 2023

RETURN PROPOSAL NO LATER THAN: July 21st, 2023 AT 5:00 PM CENTRAL TIME (END DATE)

OFFERORS ARE ENCOURAGED TO RESPOND ELECTRONICALLY THROUGH THE CITY'S E-BIDDING WEBSITE BUT MAY RESPOND BY HARD COPY (See Mailing Instructions Below)

MAILING INSTRUCTIONS: Print or type **Solicitation Number** and **End Date** on the lower left hand corner of the envelope or package. Delivered sealed proposals must be in the Purchasing Division office (701 E. Broadway, 5th Floor) by the return proposal date and time.

	(U.S. Mail)		(Courier Service)
RETURN PROPOSAL TO:	**CITY OF COLUMBIA PURCHASING** **PO BOX 6015** **COLUMBIA MO 65205**	**or**	**CITY OF COLUMBIA PURCHASING** **701 E. BROADWAY, 5th FLOOR** **COLUMBIA MO 65201**

CONTRACT PERIOD: Effective Date of Contract through One (1) Year

DELIVER SUPPLIES/SERVICES FOB (Free On Board) DESTINATION TO THE FOLLOWING ADDRESS:

City of Columbia, Public Works Department
701 E. Broadway
Columbia, MO 65201

The offeror hereby declares understanding, agreement and certification of compliance to provide the items and/or services, at the prices quoted, in accordance with all requirements and specifications contained herein. The offeror further agrees that the language of this RFP shall govern in the event of a conflict with their proposal. The offeror further agrees that upon receipt of an authorized purchase order from the Purchasing Division or when a Contract is signed and issued by an authorized official of the City of Columbia, a binding contract shall exist between the offeror and the City of Columbia.

SIGNATURE REQUIRED

OFFEROR NAME
ETA Transit Systems
MAILING ADDRESS
7700 Congress Ave, Suite 2201
CITY, STATE, ZIP CODE
Boca Raton, FL 33487

CONTACT PERSON	EMAIL ADDRESS
Nicole Castonguay	ncastonguay@etatransit.com
PHONE NUMBER	**FAX NUMBER**
(800) 382-0917	
OFFEROR TAX FILING TYPE WITH IRS (CHECK ONE)	
X Corporation ___ Individual ___ State/Local Government ___ Partnership ___ Sole Proprietor ___IRS Tax-Exempt	
AUTHORIZED SIGNATURE	**DATE**
Nicole Castonguay	july 18, 2023
PRINTED NAME	**TITLE**
Nicole Castonguay	CEO

Addendum # 1

This page was intentionally left blank.

NOTICE TO OFFERORS
ADDENDUM #1
RFP #128/2023

Offeror shall note the following information in regard to the above Request for Proposal and *incorporate this information in their submittal*. Offerors shall attach a signed acknowledged copy of this addendum to their bid response.

The RFP document has been revised to include Exhibit H – Technical Requirements.

ACKNOWLEDGEMENT OF ADDENDUM #1

The undersigned Respondent hereby certifies that the information set forth in this Addendum #1 has been incorporated in their proposal and are a part of Request for Proposal No. 128/2023. All other provisions of the proposal documents, except as herein stated, shall remain in force as written.

Firm ETA Transit Date 08/08/23

Signed Nicole Castonguay

Addendum # 2

This page was intentionally left blank.

NOTICE TO OFFERORS
ADDENDUM #2
RFP #128/2023
INTELLIGENT TRANSPORTATION SYSTEMS (ITS) SERVICES

Offeror shall note the following information in regard to the above Request for Proposal and *incorporate this information in their submittal*. Offerors shall attach a signed acknowledged copy of this addendum to their bid response.

The City received the following requests for clarification. The answers are listed below.

No.	Question	Answer
1	Please provide a current Go CoMo Fleet List including Year, Make, Model and Length of vehicles to aid in equipment installation planning.	2010 40’ Gillig (5), 2011 35’ Gillig (1), 2011 40’ Gillig (3), 2012 35’ Gillig (4), 2012 40’ Gillig (2), 2015 40’ (Gillig CNG (2), 2020 40’ Gillig CNG (1), 2020 30’ BYD K7 (4), 2021 35’ Gillig CNG (2), 2023 35’ Gillig CNG (2)
2	Please confirm the requirement for the ITS system to be integrated with the separate Automatic Passenger Counting (APC) system currently being procured as RFP 130/2023.	Yes, we will need a system that will integrate with a separate APC system
3	Please confirm if there are any existing on-board systems that the new ITS system will need to interface with (e.g., destination signs, passenger displays, audio amplifier, internal/external speaker, 2-way or VOIP radio, mobile router, APC sensors, OBDII / Can bus, onboard camera system, farebox, electronic fare collection system, etc.).	Our current system integrates with our passenger displays and internal/external speakers, mobile router and APC’s. The destination, fare boxes and cameras are currently all separate.

4	Can you confirm the number of vehicles that need to be outfitted under this solicitation? Is it the full fleet or just the fixed route vehicles?	All of the buses are to be fitted. The paratransit vehicles will not be.
5	Is City of Columbia open to a system built in response to this RFP, but designed for broader consumption, in other words, a Development Partnership?	We are open to all options.
6	What are Go CoMO's intended specifications referenced here: "System must be customizable to Go COMO's specifications"	We would like the app and landing page to reflect what we would like others to see.
7	What existing infrastructure (Make, Model, Specs) owned by City of Columbia are in place today? - Related: What is the drivers console (interface) today? Is that a laptop, tablet, iPad, etc.?	Our existing infrastructure includes the mobile routers (airlink np70), the interior head signs, drivers tablet (GTAC), passenger counting sensors, AVA equipment (through the speakers and GTAC)
8	How is connectivity managed between your buses and central dispatch? Do you anticipate this connectivity being incorporated into the solution? Or do you plan to provide connectivity separately?	We use 2 way radios and track the buses on our landing page. We will continue to use these measures. The landing page must be provided by our ITS company.
9	How many individuals need to be trained on the use of the system?	We have 14 with access currently.
10	LICENSES "Licenses - The offeror should submit a copy of all licenses and/or certifications, related to the performance of the services required herein that are held by the personnel proposed to provide such services. If not submitted with the proposal, the City of Columbia reserves the right to request and obtain a copy of any license or certification required to perform the	No requirements, just any licenses or certifications that the contractor has that may relate to the scope of work.

	defined services prior to contract award." QUESTION: Please specify the licenses the City of Columbia requires the vendor to supply. Is the vendor required to have the licenses prior to deployment?	
11	SCOPE OF SERVICES "System must be customizable to GoCOMO's specifications." QUESTION: Please give us the details of the GOCOMO specifications.	GoCOMO needs to be able to make adjustments to routing as necessary without contacting the vendor, e.g. making detours due to road construction on an 'as needed' basis.
12	APPLICATION (APP) "System shall, for passenger convenience, offer a method to integrate with the City's existing MyCoMo mobile app and/or offer a mobile app for Apple and Android devices." QUESTION: Please specify in detail the integration requirement between the ITS system and with the City's existing MyCoMo mobile app.	In most cases we can link to mobile friendly pages on any website (yours or ours). We can also utilize iFrame. All content must be at ADA compliance levels as outlined in the technical requirements document.
13	FUNCTIONAL REQUIREMENTS A.1.12 QUESTION: Would the City be willing to accept, as a way to avoid the cost of establishing and maintaining a Software Escrow Account, and to provide continuity of service to the City (in lieu of a Software Escrow Account) that upon the City's written notice, we furnish	The City would be willing to accept as long as this process is vetted by our legal department.

	transition services from the Hosting provider to the City. This includes but is not limited to, software, databases, processes, services, hardware, communications, and data and records. If transitioning to another Hosting provider this includes, but is not limited to, databases and historical records. At the time of transfer, the City would also receive a copy of the databases and historical records. The purpose of this In-sourcing (Path-Back) would be to give the City the ability and the means to transition the Hosted services back to the City or to another Hosting provider.	
14	Shall all submitters include pricing for 10% spare equipment?	No
15	Does the agency want the CAD/AVL system to integrate & provide single sign on (SSO) with signage on the bus such as the Head sign and interior signage?	A SSO is not necessary. We currently do not have SSO.
16	Does the agency want the CAD/AVL system to integrate and provide SSO with a farebox system?	It is not necessary.
17	Can proposers respond to both the ITS RFP #128.2023 and the APC RFP # 130.2023 in a single proposal or does the agency prefer separate proposals?	Please respond in separate proposals.

18	How many vehicles are available for installation at any given time?	3-5
19	Have you established a preliminary budget or budget range for this project? If so, are you able to share the budget?	No
20	In addition to using the supplied pricing sheet, may vendors also submit pricing in their own format (to mitigate confusion)?	Yes. We just ask that you use the supplied pricing sheet as it is easier for us to compare proposal pricing for each contractor. In the event that line items do not match or cannot be compared, those items may be removed from the cost evaluation and evaluated subjectively within the method of performance evaluation.
21	The scope of work section for the ITS RFP does not contain the number of vehicles that require outfitting. Please can you confirm the number of vehicles and which vehicle types require outfitting.	25
22	In the Scope of Services section (on page 6), the RFP states: ***Automated Voice Annunciation (AVA)*** • *System must be able to perform audible and visual announcements of bus stops inside the bus, as well as audible announcements outside of the bus by use of speaker system.*	42 signs total (we use them at timed stop points only)

	We take this to mean that the Contractor shall supply both a Voice Annunciation and Passenger Signage system, but nowhere else in the RFP does it specify that signage should be provided. Is it possible for the City to clarify this in the upcoming Addendum? In order to ensure you evaluate pricing on comparable scope of work, it would be ideal to have a specific quantity of signs and all of the other equipment that the City would like the vendor to install.	

ACKNOWLEDGEMENT OF ADDENDUM #2

The undersigned Respondent hereby certifies that the information set forth in this Addendum #2 has been incorporated in their proposal and are a part of Request for Proposal No. 128/2023. All other provisions of the proposal documents, except as herein stated, shall remain in force as written.

Firm ETA Transit Date 08/08/23

Signed Nicole Castonguay

Firm profile, capabilities, & experience

[What you will discover]

ETA Transit finds itself squarely positioned as the 'best of both worlds' transit technology provider. Ours is a company whose origins date back to the mid-1990s as GeoFocus—a pioneer in the rail tracking and passenger information industry. From those beginnings, our evolution has seen us adapt our product offerings to meet the challenges of a modern transit industry by embracing the latest technology and development methodologies.

[Section key points]

- Expertise: ETA Transit leverages its rich history in the public transit and university shuttle tracking with the latest technology and best practices to provide an unmatched balance of industry-specific wisdom, proven performance, and innovation to the City of Columbia.
- Ingenuity: Ours is an experienced team boasting over 200 years of combined experience across multiple transportation, technology, and business disciplines which provides GoCOMO the confidence to know that ETA can and will deliver a successful project
- Referrals: Backed by a history of accomplishment, highlighted by a consistent record of retaining customers and delivering exceptional service in diverse transportation markets such as transit and university transportation. GoCOMO can be confident that choosing ETA is a decision founded on a legacy of proven success

Meet the team!

The difference maker in this decision has been the dedication of the ETA Transit team in all phases of this project."

— Maureen Coughlin, Senior Facility Manager, SP+

About

ETA Transit Systems, Inc. provides intelligent transit solutions (ITS) to public transportation, airport parking operations, university, corporate campus, medical facilities, car rental companies, and theme park companies across the United States. Its flagship ITS platform, SPOT™ provides real-time CAD/AVL tracking, data collection, reporting and analytic, and related traveler information systems to a variety of stakeholders, including transit agencies, departments of transportation, and passengers.

Corporate address: 7700 Congress Avenue, Suite 2201, Boca Raton, FL 33487
Phone: (800) 382-0917
Website: etatransit.com
Email: sales@etatransit.com

Our mission statement

Providing the industry's best intelligent transit systems is not a destination; it is a journey, a mission that requires an openness to new ideas, adoption to the latest practices and technology, and deliberate, focused attention to providing fanatical service.

This journey demands a relentless pursuit of innovation to ensure our customers have a partner; a critical, indispensable resource in their operations.

The long-term value we create defines our success; and the respect and trust we earn, and our dedication to extending our triumphs to every corner of our operations so that every contributor will benefit from our efforts.

DBE status

ETA has been a woman-owned business since 2013. Nicole Castonguay, ETA's Chief Executive Officer (CEO), owns 65 percent of the firm's common stock and is responsible for all day-to-day management decisions and for implementing the company's long- and short-term plans. Ms. Castonguay acts as a direct liaison between the board and management of the company. She communicates to the board on behalf of management.

- WBENC national certification: 2005129289
- Expiration date: 7/22/23
- NAICS codes: 541512, 541511, 541519, 518210, 485111
- UNSPSC codes: 25170000, 81112501

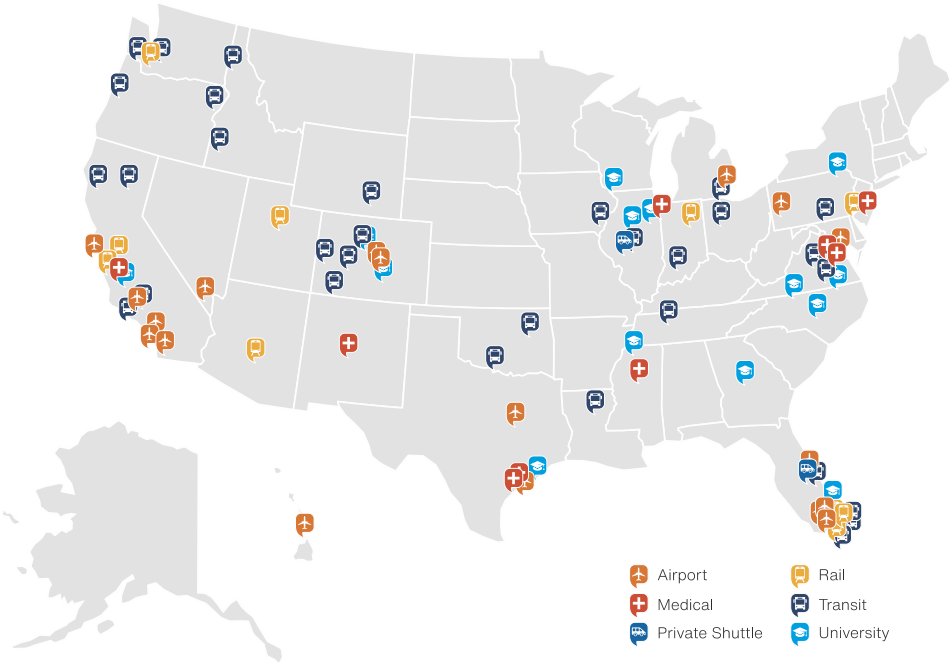
History

As one of the pioneers of modern, cloud-hosted ITS systems, our origins in transit can be traced even further to the mid-1990s and the legacy rail tracking platform, TrainTrac™, by GeoFocus®. ETA Transit has been at the forefront of location-based intelligent transit technology since it purchased GeoFocus® and subsequent relaunch as ETA Transit Systems in 2003.

Unlike many recent upstarts in the transit technology space, our history delivers a track record of proven performance, adaptability, and multi-modal transit solutions that spans over a quarter of a century across hundreds of successful deployments across the United States.

Customers

ETA Transit has over 80 highly satisfied customers spanning the United States and multiple transit industries. This diversity in customers speaks to the flexibility of the SPOT™ ITS and its ability to deliver right-sized solutions, and long-term viability of ETA as a transit partner to GoCOMO.



A legacy of partnership:

Public transit

Shuttle, university, and campus transportation

References

Highly satisfied ETA customers

We encourage our potential transit partners to contact current customers for real-world feedback about ETA, SPOT™, and our customer support. We have provided you with references of comparable size and situation to the City of Columbia, but please feel free to reach out to any of our other clients. We will be happy to provide you with their contact information upon request.

1) Valley Regional Transit

Type of business:	Public transit
Contact person/title:	Nick Moran, IT Director
Telephone:	(208) 258-2713
Email:	nmoran@ridevrt.org

---

2) Toledo Area Regional Transit Authority

Type of business:	Public transit
Contact person/title:	Lucas Boehm, Director of Information Technology
Telephone:	(419) 245-5226
Email:	lboehm@tarta.com

---

3) AppalCART

Type of business:	Public Transit/University Transportation
Contact person/title:	Craigh Hughes
Telephone:	828-297-1300 ext. 104
Email:	director@appalcart.com

Partnerships

The key to meeting the current and future needs of the market

Developing and maintaining strategic relationships is one of the cornerstones of ETA's business development strategy. These partnerships help us stay abreast of changes in the market, stay at the forefront of emerging technologies, identify new customers, facilitate integration capabilities, and deliver competitive price options to our customers.

We have long understood the importance of these mutually-beneficial relationships and actively seek out opportunities to support our partner companies. We provide them with first-looks at new products, engage them in the product development and testing process, and provide special considerations for pricing, deployment, and support.

Original equipment manufacturers

BYD · GILLIG · NEW FLYER · ELDORADO

Technology partners

SPOT™ integrates with every major transit software solution provider to provide TANK with the ability to add, upgrade, or transfer functionality from their current ITS provider to a SPOT-powered system.

DAKTRONICS · DILAX · Fleetio · KELLA · LUMINATOR TECHNOLOGY GROUP · optibus · orion · PAPERCAST® · remix · SEON · spare · transit · TransTrack SOLUTIONS GROUP · Ubisense · VIRICITI · WAYSINE

Daktronics®

Daktronics® is a longtime partner with ETA and has delivered competitive pricing on large transit signage and displays for our transit and airport projects. Our relationship extends over 20 years and includes high-profile installations for Amtrak, Tri-Rail, and more.

Fleetio®

Our preferred partner for trip inspection, Fleetio®, delivers an incredible package of incident management solutions that genuinely deliver that convenience and capability that frees transit agencies from manual

processes. Armed with ETA's handheld inspection device, drivers and maintenance personnel can easily log issues, report incidents, and notify vehicle support teams of pressing performance concerns.

Hella®

ETA was the first transportation technology company to realize the capabilities of Hella® automatic passenger counters and deploy these 98-percent accurate systems to dozens of transit agencies across America. It's a partnership that extends over a decade. We're the first to learn about new products, receive preferred pricing, and actively contribute to product development on new and more powerful counting technologies.

Luminator®

Luminator Technology Group delivers globally recognized technology solutions that increase intelligence, safety, and efficiency for public transit operations. Luminator® is uniquely positioned to provide solutions to connect transit passengers to vital information while supporting the operational objectives of efficient transit operations. Supporting transit bus and rail car manufacturers as well as public transit operators around the globe, Luminator is developing and delivering technology with tangible benefits to public transit.

Optibus®

Our partnership with Optibus® features two high profile collaborations: Facebook and Ft. Lauderdale International Airport. In both instances, this integration shares data that provides real-time operational information to the Optibus® optimization engine and delivers a standardized GTFS feed to connected traveler information and planning systems.

Orion®

Orion® delivers a compelling, state-of-the-art voice-over-internet phone (VOIP) system that frees our customers from their reliance on outdated and sometimes frustrating radio technology. The Orion system is a game-changer for the transit industry and integrates perfectly with our SPOT™ ITS.

Papercast®

ETA has been the sole North American provider of Papercast® digital e-paper displays for the last two years. What started as an exploration into alternatives to current e-paper solutions evolved into a strong partnership with joint branding and marketing efforts, product testing, and mutual promotion of our respective products.

Remix®

Remix is the first planning platform for public transit. Design, evaluate, and collaborate all in one place — from a small detour to a full system redesign and everything in between. Quickly test out new ideas, evaluate impacts, and iterate. Remix's public transportation planning software makes it easy to see the trade-offs of how proposed changes impact your network.

Seon®

Manufacturing world-class video surveillance systems for school bus and public transit, Seon helps transportation managers capture, record, view, and wirelessly download on-board security footage, quickly and reliably. Fleet management solutions such as live vehicle tracking, passenger ridership tracking, and school bus routing are integrated with mobile video to give fleet managers real-time information about their fleet operations—for total fleet awareness.

Spare Labs®

Spare Labs® solves the demand-response and paratransit needs for any transit operation who needs to satisfy the transportation needs for challenged members of its service area. Their powerful solution delivers secure collection and storage that conforms to HIPPA requirements, scheduling, routing, on-demand service, rider apps, manages payment and insurance information, and much more.

Transit App®

Transit App dreams of happier communities, where multiple modes work together and getting from A to B with Transit is simpler than climbing into a car. Our cities came long before the car and will still be around after all the cars are gone. They are a team of developers, designers and transit nerds who believe technology can make sustainable transport more popular than ever. Whether it's public transit or bike sharing, we believe the revolution taking over our streets will be captained from our phones.

TransTrack®

TransTrack Systems® provides a web-based transit business analytics and data management system to efficiently aggregate data from multiple sources for enhanced performance monitoring and reporting.

The solution acts as a system consolidator or data warehouse focused exclusively on key transit agency information for display using business analytics. Summary data may be imported from an existing system or entered directly into the application at either the summary or transaction level.

Ubisense®

A recent addition to ETA's stable of trusted integrations is the yard management from Ubisense®. This powerful expansion helps provide real-time location services for transit bus barns, and help agencies keep a tight eye on where a bus is located, it's current status, service condition, and more. It's an excellent solution for mid- to large-size transit operations.

Viriciti®

As the demand for real-time vehicle monitoring becomes a primary way to ensure fleet health, ETA has forged a relationship with ViriCiti®. This partnership ensures seamless integration and single point of control within the SPOT™ administration console.

WaySine®

As a preferred partner, WaySine® has partnered with ETA on several digital signage and solar-powered display projects. They are a valued resource and provide our customers with competitive pricing, proven performance, and easy integration to the SPOT™ platform.

Executive leadership team

Guiding ETA Transit is a team of highly qualified professionals with a diverse range of multi-disciplinary education, experience. This collection of talent helps to shepherd new product development, nurture customer and vendor relationships, safeguard fiscal responsibilities, and mentor staff.

Nicole Castonguay, CEO

Education:

Bachelor of Science in Business Management; University of Central Florida

- Responsible for daily operations, sales, and accounting
- Experience in customer service, operations, and accounting
- Prior: Regional Director for the Hilton Hotels Corporation®

John Maglio, President & CTO

Education:

Bachelor of Science in Finance; University of Central Florida
Bachelor of Science in Management Information Systems; University of Central Florida

- Responsible for product strategy and business development
- Experience with establishing and managing strategic relationships, operations, and the development, and implementation of mass transit products
- Prior: Director of Software Engineering for GeoFocus®

Steven Friedman, CFO

Education:

MBA Finance/Marketing; Weatherhead School of Management at Case Western University
Bachelor of Business Administration in Accounting; University of Texas at Austin

- Responsible for financial strategy and accounting
- Experience with establishing financial strategies for multiple business segments
- Prior: Senior Vice President Reichel Realty and Investment, Inc.

Stephen Gunning, Vice President of Systems & Support

Education:

MBA Business Analytics; Florida Atlantic University
Bachelor of Science in Computer Science; Florida Atlantic University

- Responsible for architecting ETA's technology systems
- Experience with extending purpose-built systems to more versatile platforms, software conversion, software engineering, operating systems, and algorithms

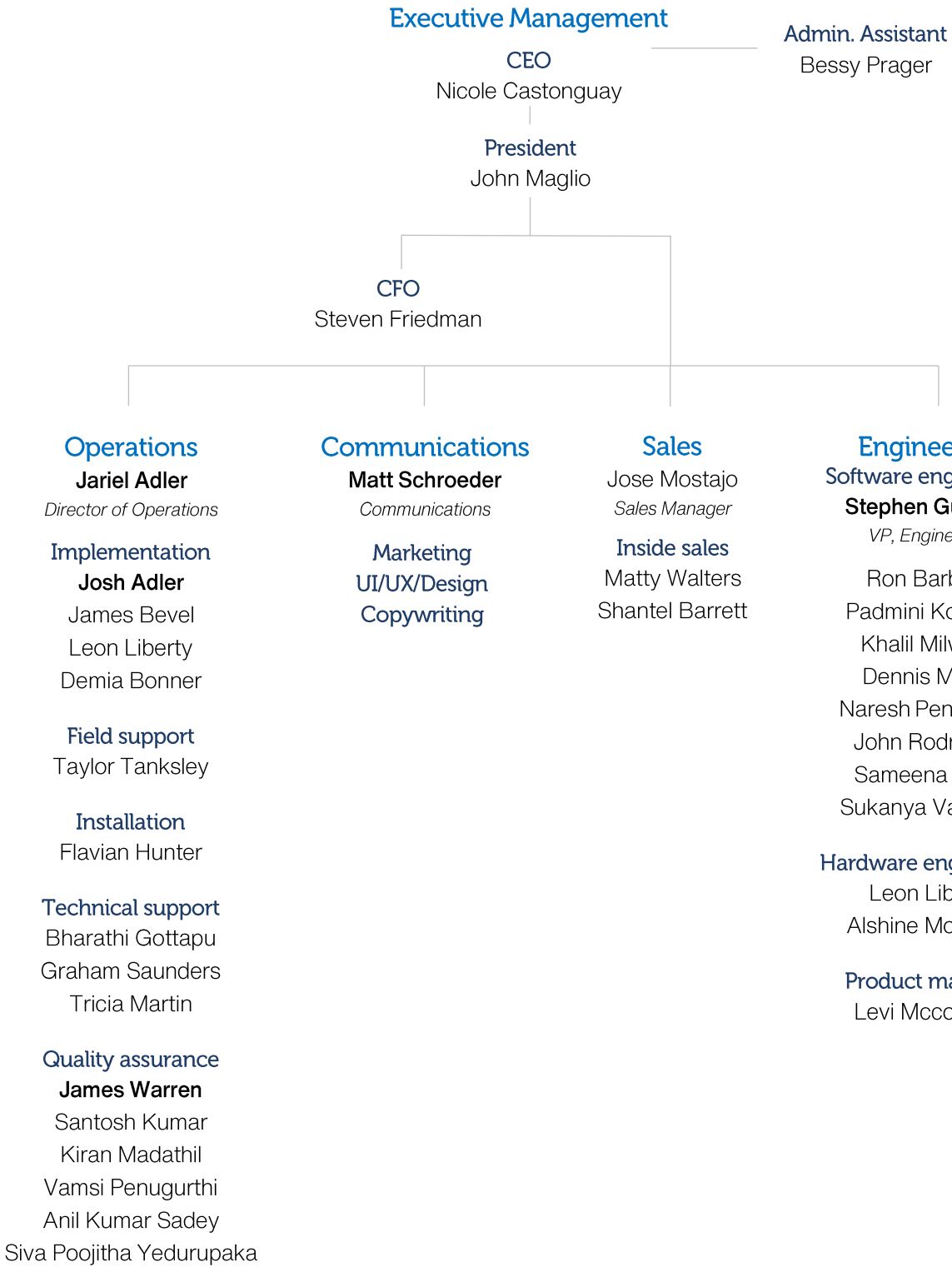
Jariel Adler, Director of operations

Education:

Bachelors in Management Information Systems; Florida Atlantic University

- Responsible for management of customer support team
- Project Management Professional (PMP) — Nov 2012 # 1551776
- Deployment Project Manager for 8 years with deployments at TBC—Tire Kingdom and Big O Tire & G4S Retail Division

Organization chart



Product & services

[What you will discover]

The proposed solution delivers a complete real-time passenger information system that will benefit GoCOMO and it's customers by providing all the tools and technology needed from a single vendor, ETA Transit. The SPOT™ system addresses the challenges of unreliable tablets and poor performing onboard integrations with a proven hardware architecture and robust technology tool set. Most importantly, the core system will be delivered in under 8 weeks from notice to proceed.

[Section key points]

- **Experience:** ETA Transit's 20+ years of experience in providing CAD/AVL hardware and technology to transit and university agencies which will ensure a smooth implementation for the City of Columbia and the 30,000 plus students the University of Missouri that use GoCOMO
- **Reliability**: GoCOMO needs a transit system that can perform reliably and accurately collect real-time which the SPOT™ system delivers by emphasizing reliable hardware with a proven architecture
- **Scalability**: The City of Columbia requires a system that can facilitate growth and expansion down the road, which the SPOT™ ecosystem can easily achieve by providing a service-oriented architecture (SOA) that allows for easy expansion and customization
- **Passenger Experience**: GoCOMO aims to provide passengers with a reliable and efficient transit experience, which the SPOT™ system can achieve through solid traveler information systems, including mobile apps and websites, station signage, and third-party application integration, to remove uncertainty from riders' travels and improve their overall experience
- **Responsiveness:** ETA Transit is committed to providing exceptional support services, with a key focus on responsiveness. Our objective is to prioritize GoCOMO by ensuring that their concerns are acknowledged and addressed promptly. Our aim is to instill confidence in the City of Columbia, knowing that ETA Transit is readily available to assist them whenever needed

Onward!

"The SPOT system delivers precisely what our customers have requested."

— Evan Wexler, Executive VP of Operations, Sixt® Car Rental

SPOT™ System overview

A cloud-based platform

SPOT™ utilizes a software-as-a-service (SaaS) deployment, or perhaps more colloquially, it is a cloud-based platform that manages the entirety of its system from a series of off-site servers. This approach provides several critical benefits over a traditional on-site solution.

- Cloud-based servers provide redundancy against outages or service disruptions
- Cloud-based servers mitigate the risk of local damage due to weather, vandalism, or other disasters
- A cloud-based approach provides anywhere-access from any Internet-connected device, such as laptops, tablets, and smartphones
- System updates, new software, and feature improvements can be 'pushed' wirelessly and automatically to on-vehicle or at-station hardware such as mobile data terminals (MDT) or digital displays
- No cost for servers or IT resources

Our cloud-based platform allows for specific system capabilities (modules) to deploy wirelessly based on specific operational requirements. It provides a clear and straightforward path for software updates and upgrades. Perhaps most importantly, it means that you are not paying for system capabilities your organization does not need.

Hosted on Amazon® Web Services™

SPOT™ hosts its platform on Amazon® Web Services™ (AWS EC2) servers to provide the maximum amount of performance, load balancing, and security across our customer base.

With different regions around the world, Amazon AWS provides ETA with the ability to host its software on servers closest to the customer service area. ETA will leverage this geographic advantage to provide the best possible latency.

Open source software (OSS)

ETA's internal software auditing program ensures that any software—open source (GPL) or commercial is properly licensed for the manner which it is used in the SPOT™ ITS system. Within the scope of the GoCOMO project the following GPS resources are used:

- JScolor.js
- HighCharts.js

All other libraries are licensed as permissive under Apache 2.0 or MIT. A full listing of all OSS software is in Appendix D: Open-source software.

Open architecture design

SPOT™ is a service-oriented architecture (SOA), which provides extensive access to its system services for 3rd party developers and allows for easy integration and expansion of new capabilities. Built on open-data standards, ours is an approach that is critical in any leveraging existing systems and reducing initial investment expenditures.

The SPOT™ ITS supports data exchange using non-proprietary industry standards such as GFTS and JSON-based web services.

This approach is critical in maximizing both existing onboard hardware and ensuring an easy path to upgrading the system in the future. A SPOT-powered system does not have to be implemented all at once. ETA's approach to system design provides our clients with unparalleled freedom to add new features down the road, or gradually implement growth plans over a period to maintain financial flexibility.

Active development process

The SPOT™ system you purchase today will not be the same system you use next year. That is because ETA has adopted an active and iterative development process. Our design philosophy is centered around providing a stable and feature-rich platform that continually improves upon its capabilities.

The software engineering team releases new performance updates, security patches, and system enhancements every two weeks. As we develop new features or functionalities to subscribed systems, our customers can expect to receive these improvements at no additional charge.

Third-party integration

Hardware

The SPOT™ platform easily integrated with most hardware systems used in transit operations. We frequently integrate with:

- Automatic fare collection systems (Genfare®, Masabi®, Umo®)
- Automatic passenger systems (Hella®, Iris®)
- Digital display systems (Daktronics®, Luminator®, Sunrise®)
- Mobile video surveillance systems (Apollo®, REI®, Seon®)

- Onboard public address systems
- Onboard Wi-Fi routers
- Solar-powered LED and E-Paper displays (Papercast®, Waysine®)
- Vehicle LED head sign and wayside signage

If not included within the initial RFP documentation, a listing of all parts (make, model, etc.) will help identify compatibility concerns. A hardware audit will be conducted as part of ETA's pre-project on-site deployment survey to help identify potential issues. See section on implementation strategy for more information.

Software

SPOT™ can successfully integrate with most third-party solutions, including on-demand systems, microtransit solutions like Uber® and Lyft®, and even competitor software for scheduling, paratransit, self-serve analytics, TransitApp®, and more. All that is required is a vendor-supplied API for us to consume data from the source system. Once connected, these systems can be integrated into the SPOT™ back-office interface for a convenient, single-source access point for connected systems. Among our integration partners include:

- Fleetio® fleet management
- Optibus® scheduling
- Orion® VoIP communications
- Remix® planning
- Spare Labs® paratransit
- TransTrack® business intelligence
- Ubisense® yard management
- ViriCiti® (Chargepoint®) vehicle inspection

API access

Flexibility is a core component to the SPOT™ platform, and what better way to ensure that our customers have the freedom to develop custom solutions than by providing unfettered access to the same API our staff uses to create new features and capabilities? We will happily supply your developers with the resources and documentation needed to develop your additions to your SPOT™ deployment.

Commercially available off-the-shelf hardware (COTS)

ETA has embraced a philosophy of utilizing commercially available hardware as opposed to developing its brand of proprietary equipment. This approach provides many critical benefits:

- The commercial nature of the product means an abundance of supply and increased options for accessories, such as secure mounts, cases, and connectivity features
- The equipment has been subjected to rigorous testing and passes thorough quality standards.
- The product is likely to be familiar to the public in terms of functionality
- It leverages the cost-advantages found in mass-produced products, providing for a lower cost of ownership and more stable supply chains
- Widespread availability provides for quicker and easier replacement and upgrades
- High mean time between failure (MTBF)

These advantages free transit agencies from the reliance on proprietary solutions that put them at the mercy of their vendor and its supply chain, resulting in less downtime due to equipment failure and a quicker path toward recovery.

Rigorously tested hardware

We subject all our hardware to extensive testing in our in-house hardware lab. We test the exact configuration of your system components using the same hardware and software (down to the same wires, fuses, and mounting screws) that will are on your vehicles. We identify potential points of weakness and take the appropriate steps to minimize the risk of on-site issues that may adversely impact deployment timelines.

Data collection

The essential item for effective use of any intelligent system is access to the data gathered during normal operations. The construction of SPOT™ provides a measure of redundancy for the continual collection of this valuable information. The onboard vehicle logic unit or tablet continues to collect data while the vehicle is in operation. This information will automatically be uploaded to the system once the connection is re-established. ETA will store and make available all collected data for the life of your contract—without any additional access fees.

System security

Security is of paramount concern to ETA Transit. The data of the City of Columbia (and their clients) remains protected by up-do-date security practices, secure from outside entry. We never divulge

confidential information to third parties, so the names, contact information, and system data remains safe and private; accessible only by those to whom you grant access.

All ETA systems are protected by firewall ACLs. We limit open ports to only those required for essential system operation with a quarterly rotation of all system passwords to enhance overall security.

The User Manager module found within the SPOT™ Administration Console provides password- and role-based security on an individual level, to ensure that staff have access only to those parts of the system relevant to performing their duties.

Disaster recovery

SPOT's cloud-hosted nature provides an incredible benefit when dealing with unexpected server and connectivity issues. Should a server encounter hardware or connectivity issues, SPOT™ services are re-routed to a redundant server.

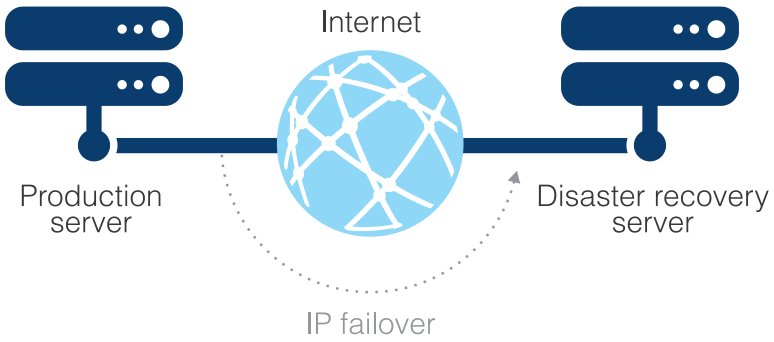


Figure 1: IP failover with RTO 60 minutes with TTL set to 60.

All information regarding your operations is backed up in real-time, providing an added layer of disaster recovery. If desired, ETA can also configure automated daily downloads of your transit data to a local server at your location via a secure FTP connection.

Turnkey system

ETA provides a turnkey solution that does more than introducing innovative technology to your transit agency—we provide on-going, comprehensive system support, including:

- On-going training to improve staff comprehension and get new hires up-to-speed
- Trend analysis to help you maximize your system and organizational performance

- Proactive system monitoring to alert you to potential issues
- Online reference and support materials to help train, educate, and troubleshoot problems
- A dedicated Customer Experience Advocate (CEA) to help guide, mentor, and find solutions
- Live online chat with our support team
- Go-to-market materials and strategies to help generate excitement among staff and riders
- A single point of contact to assist you when issues arise

Modular system deployment

A foundational principle found in the SPOT™ platform is one built on the idea that an investment in an ITS solution should meet an operation where it currently exists and evolve with it over time.

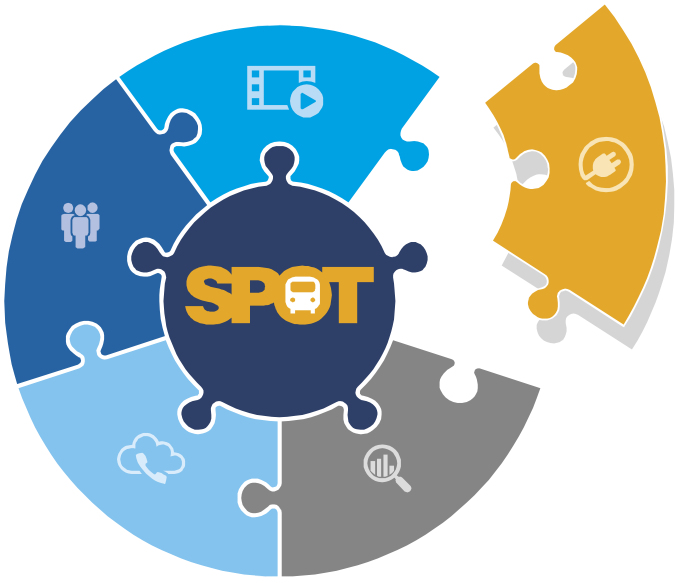


Figure 2: New modules are easily 'plugged' into the SPOT™ system to create a customized, 'right fit' solution that delivers precisely the tools and resources needed to meet specific operational goals.

SPOT™ is highly adaptable. Our customizable ecosystem of software modules and integration capabilities meet the needs of any transit agency. This approach provides an unparalleled level of customization and ensures that the City of Columbia precisely deploys the tools it needs to succeed. Many of these features can be quickly deployed wirelessly without the need for on-site configuration.

Standard capabilities

The SPOT™ system delivers a unified platform for simplicity of management, integration, and overall efficiency. The SPOT™ base package delivers exceptional out-of-the-box performance with key features and tools required by most transit operations, including:

- Automatic vehicle location
- GPS tracking
- Over 100 built-in reports for on-time performance, ridership, NTD, and fleet management
- Route manager with detour management and GTFS and GTFS-R import/export
- Service messages
- Station content management
- System configuration utility
- Electronic passenger counting
- Driver messaging
- User management
- Branded public-facing tracking websites and mobile apps
- Go-to-market support materials and strategies

The SPOT™ platform also provides a graduated means of evolving onboard systems to match budgetary and operational goals. For example, a smaller agency in a growing community might not immediately require a complete ITS system with installed onboard hardware—but it does need a path for rapid expansion once the demands of its service area grow as a result of increased population and infrastructure.

Expansion and customization options

SPOT™ and its modular design provide a streamlined path toward customization and feature enhancements, upgrades, and expansion. ETA currently provides solutions for:

- Automatic Passenger Counting (APC)
- Automatic Vehicle Announcements (AVA)
- Automatic Vehicle Monitoring (AVM)
- Business Intelligence (BI)
- Electronic fare collection
- Infotainment
- Mobile Video Surveillance (MVS)
- Onboard Wi-Fi
- Paratransit / Mobility
- Passenger Information Displays (PIDS)
- Pre-Trip Inspection
- Q-straint® Quantum™ integration
- Solar-powered e-paper signage
- Voice Over Internet Protocol communication (VoIP)
- Custom 3rd party system integration

Traveler information systems

Figure 3: Figure 9: Public tracking website (left) and mobile app (right) for Android™ and iOS™.

Vehicle tracking information applications are cornerstones of any ITS solution, and SPOT™ delivers a versatile platform with the following standard features:

- Large, two-dimensional maps with traditional and street view options
- Multiple route selection
- Real-time arrival predictions for any vehicle or stop
- System alerts and messaging
- Color-coded routes
- Responsive display scaling and touch screen support
- Smooth vehicle tracking with color-coded status icons (late, on-time, early, etc.)
- Collapsible navigation
- Custom rider alerts and favorite stop/route selection
- Trip planning tools with local attractions (banks, shopping, restaurants, etc.)
- Detailed vehicle and station information

- Station amenity details (lighting, schedules, stop images, etc.)
- Rider feedback
- Passenger engagement tools for advertising, promotion, branding, surveys, and more
- Mobile app download links
- Real-time URL access for high-definition smart LCD station displays
- Help and tutorials
- Branded with logo and custom colors
- Option for custom, agency-branded standalone mobile app

Take the app for a test drive!

Curious how our app stacks up to the competition? Download the SPOT™ mobile app and give it a test drive to try out all its features using data from a current ETA Transit partner agency.

SPOT™ system architecture

[What you will discover]

SPOT™ delivers an incredibly powerful ITS solution and the freedom to configure your system to deliver precisely the tools and features required to meet the challenges of the GoCOMO's operations.

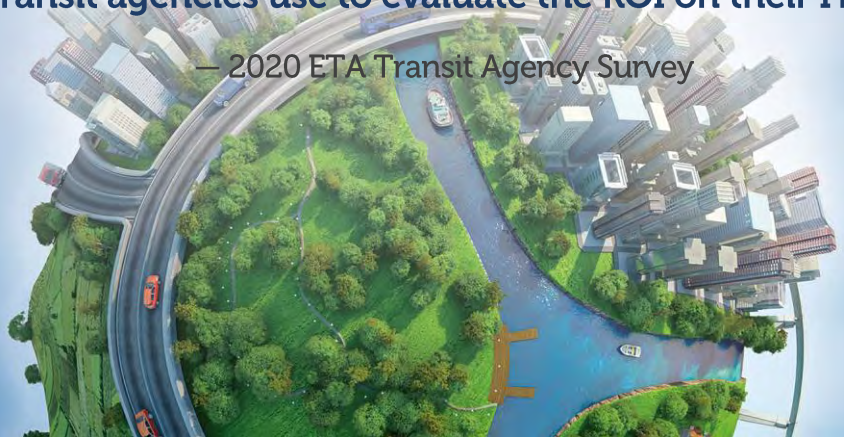
[Section key points]

- Fault Tolerant Design: With SPOT's hardwired design of a separate Vehicle Logic Unit (VLU) and Mobile Data Terminal (MDT), GoCOMO will deploy a resilient design that mitigates risk and ensures accurate data reporting
- Modular Design: The modular design of SPOT™ enables a streamlined path for the City of Columbia towards enhancements, upgrades, and expansion such as Automatic Passenger Counting (APC), Automatic Vehicle Announcements (AVA), and Mobile Video Surveillance (MVS)
- Professional Installation: The use of pre-fabrication techniques ensures that the components of the system are manufactured to high-quality standards, reducing the potential for errors during the installation process allowing GoCOMO to focus on their core operations

Start your engines!

Increased staff efficiency (64%), an improvement in schedule performance (61%), and accurate reporting (59%) rank as the top three areas transit agencies use to evaluate the ROI on their ITS system.

— 2020 ETA Transit Agency Survey



The SPOT™ automatic vehicle location (AVL) system

At the heart of our SPOT™ ITS is the capability to track a vehicle across any location accurately. We accomplish this by combining our rugged, transit-tested hardware with a pre-deployment GPS/cellular survey to identify potential gaps in coverage. The reliability of hardware and cellular coverage are critical components in the collection of the vehicle location and transit-related data that is essential to the accurate conversion of operational information into usable transit information.

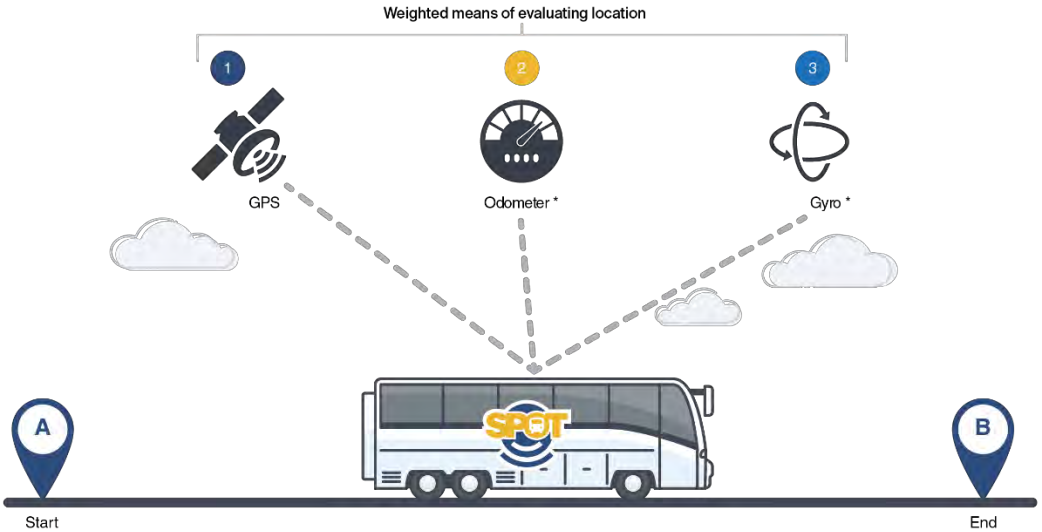
SPOT™ natively supports the following cellular providers: AT&T, T-Mobile, and Verizon

An intelligent, learning platform

The longer a SPOT™ system is in service, the more precise its arrival predictions become. It adjusts its arrival predictions based on established history and performance information, including schedules, time of day, weather conditions, and other factors. Here is how it works:

The SPOT™ location engine

The SPOT™ platform utilizes global positioning systems (GPS) to determine vehicle location and passes the data over to the SPOT™ arrival prediction engine. In most operations, GPS data is ideal for collecting valuable position and location information about a vehicle. If required, a SPOT™ ITS system can overcome these limitations by adding RFID sensors, gyroscopes, dead reckoning systems. The SPOT™ ITS intelligently evaluates the dependability of GPS inputs based on the signal strength and the number of available satellites.



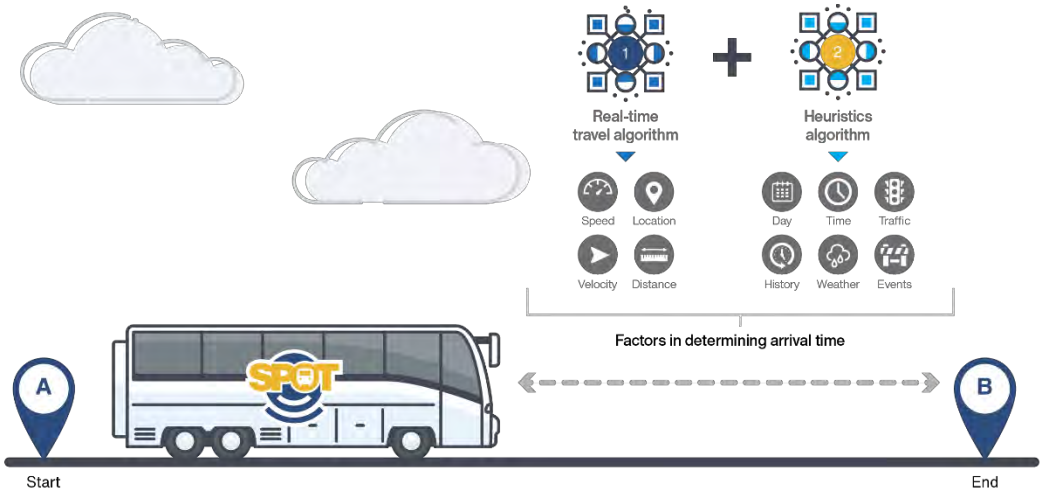
* Optional components. *Not available on SPOTLite™ systems.*

The SPOT™ arrival prediction engine

Using the current position provided by the location engine, the ETA arrival prediction engine attempts to calculate the estimated time of arrival to the next stop using two methods:

- A real-time travel algorithm based on location, speed, velocity, and distance
- A heuristics algorithm that defines a travel profile based on numerous criteria including day, time, and average run time over similar profile periods.

When location data is combined with the travel algorithm and heuristics data, a highly accurate arrival prediction is obtained and can be provided to connected systems.



The SPOT™ delivery service

Once the arrival prediction calculates, the data transmission delivers to every down-stream system, including onboard announcements, digital signage, CAD/AVL software, reporting systems, bus tracking websites, and other rider alert subsystems. This transfer of information happens automatically, negating any need for manual action to display system data to connected devices.

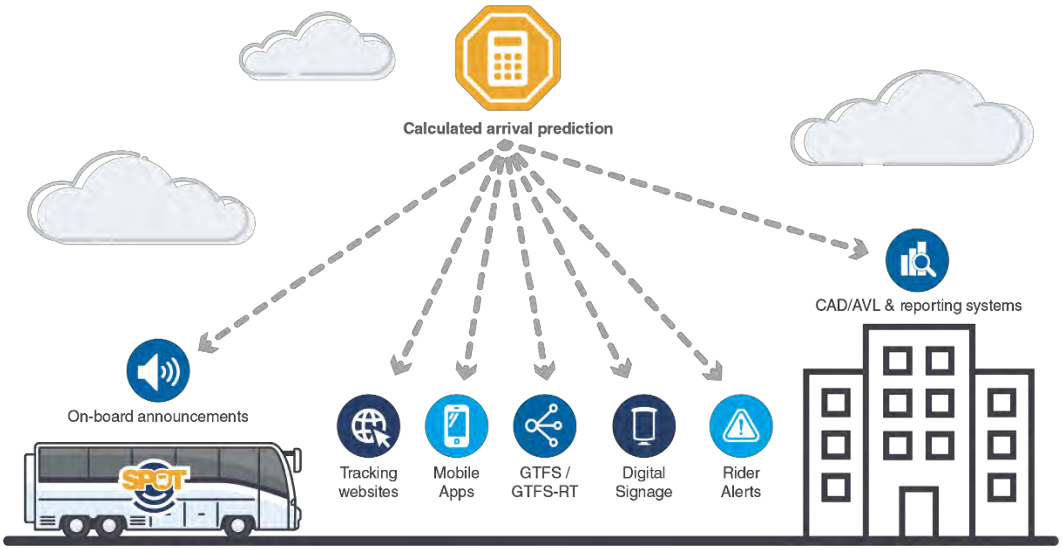


Figure 4: Real-time travel data automatically transmits to all connected systems within your transit operations.

Separate MDT and VLU construction

Your SPOT™ ITS will utilize a construction that features a separate Mobile Data Terminal (MDT) and Vehicle Logic Unit (VLU). The primary reason for this approach to system design over an all-in-one tablet is both apparent and vital—*to protect your data*.

A fault-tolerant design

ETA's system design delivers a more fault-tolerant solution and mitigates the single point of failure that can occur in an all-in-one system. Our design secures the heartbeat of your SPOT™ system (the VLU) away from potential harm. It protects it from jostling passengers, bumps from a stray umbrella, the prying fingers of a curious kid—all real concerns from an all-in-one hosted system that is out in the open and within reach of any number of potentially damaging risks.

With an all-in-one solution, if the hardware ceases to function, all information collection and tracking ceases. A separate MDT/VLU system can continue to operate, collect, and transmit data and control onboard systems—*even if the MDT is damaged*.

Table 1: High-level comparison between separate MDT/VLU and all-in-one system design.

Separate MDT and VLU construction		All-in-one construction	
Advantages	Disadvantages	Advantages	Disadvantages
MDT failure does not impact ITS functionality	Non-plug and play VLU	Plug and play	Single point of failure

Higher powered computer	Higher initial adoption cost	Lower initial adoption cost	Lower powered computer
More connectivity options			Fewer connectivity options
Secure wiring to connected systems			Exposed wiring to connected systems
Non-proprietary hardware			Proprietary hardware
No chance of VLU theft			High chance of theft
Minimal risk of a supply chain disruption			Higher risk of a supply chain disruption

More power

The separate MDT-VLU approach provides greater possibilities for long term expansion. The SPOT™ VLU is a highly capable, exceptionally reliable computer with enough power to drive all onboard systems, including LCDs, mobile video security, fare collection systems, and rich-media infotainment.

Expansion options

A SPOT™ system provides the maximum amount of expansion and customization features. While the base system delivers the essential tools for running a transit operation, it is the ability to add, adapt, and expand your system that genuinely defines the long-term value of this platform.

Key concept!

Protecting operational data is critical in helping define long-term growth strategies. An investment in reliable system design and components is an expense that delivers year-over-year benefits far more than the initial procurement cost.

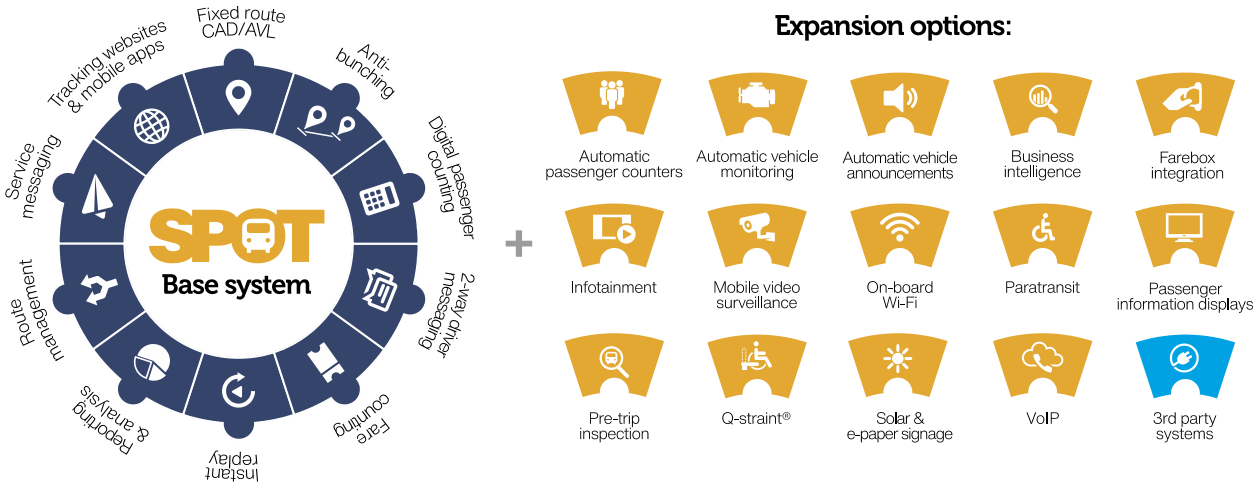


Figure 5: The SPOT™ system design provides a simple pathway to upgrade your ITS at any time.

Vehicle Logic Unit hardware

The backbone of the system, the VLU, must be a workhorse computer with the power to repeatedly deliver in a rugged, demanding transit environment. ETA's selection for the GoCOMO project is a transit-tested powerhouse that will provide years of reliable service that features:

- Intel™ Gen4™ Dual-Core 298U 1.6GHz
- 1 x DDR3L-1600 SO-DIMM up to 8GB
- Wireless support for LTE, 3.5G, WLAN, GPS, GSM, GPRS, and Bluetooth connectivity
- Support 1 x RS-232 (COM 1 with 232/422/485)
- Support 2 x DI / 2 x DO (12V/100mA)
- Intel™ HD graphics
- 3 x USB 2.0 ports; 2 x RJ45 ports
- 1 x HDMI and DVI-I
- Support two in and two out GPIO port

Figure 6: SPOT Pro™ VLU.

- Mic in / line out Audio
- 3 x mini-card slots
- 1 x 2.5" drive bay for SATA hard disk/SSD drive

Obstructed views: The VLU can be equipped with an optional gyroscopic dead-reckoning system to account geographic considerations where a clear view of the sky may be impacted, such as highly mountainous regions, tunnels, or parking garages. This system automatically maintains tracking of the vehicle and ensures the accurate triggers of onboard announcements.

Mobile Data Terminal hardware

ETA's choice for the City of Columbia's onboard MDT is a high-definition LCD touch screen display with a 7" viewable area and an impressive 170-degree horizontal and vertical viewing angle—an essential consideration to maintaining at-a-glance visibility in a variety of operating conditions. The MDT is secured to the vehicle by an articulating mount with secure hex screws to deter theft. The monitor is a 'dumb' terminal, meaning that it does not contain any software or specific operating functionality. This approach simplifies use and minimizes any potential issues that can hobble your onboard operations.

- 7" capacitive touch screen display
- 7.28" w X 4.7" h X 1.16" d
- 1920 x 1080 max resolution at 60–72Hz
- 20ms response time
- 140°x X 120°y viewing angle
- LED backlight
- HDMI, VGA, component, and composite inputs
- 1.2W speaker
- 3.5mm headphone output
- VESA 75 mounts
- Operating temp -4° – +140°F

Figure 7: Mobile data terminal and articulating mount (inset).

A safe and secure MDT

Security is a primary concern; security against theft and security of information. The SPOT™ MDT offers a secure and reliable, "locked down" platform that defends against common exploits of Google® Android™ and Apple® iOS™ devices. Our rigorous restraints of access prevent the installation of any third-party applications, like games, messengers, and ebook readers, which can serve up potential exploits that can affect the integrity of the overall system.

This heightened level of security ensures that drivers only use the MDT for intended purposes, that installed software performs as designed, and that sensitive data is protected.

Wiring harness design

The SPOT™ wiring harness mounts to a vehicle's equipment cabinet easily and securely. This strategy removes any haphazard approach to installation and ensures that maintenance teams can easily access and maintain hardware and wiring components.

Professional installation

ETA's highly-trained professional deployment teams will ensure a secure installation and configuration of your equipment on your vehicles. Their work is backed by a 60-day hardware installation guarantee that begins on the first day your SPOT™ system goes live after customer witness testing.

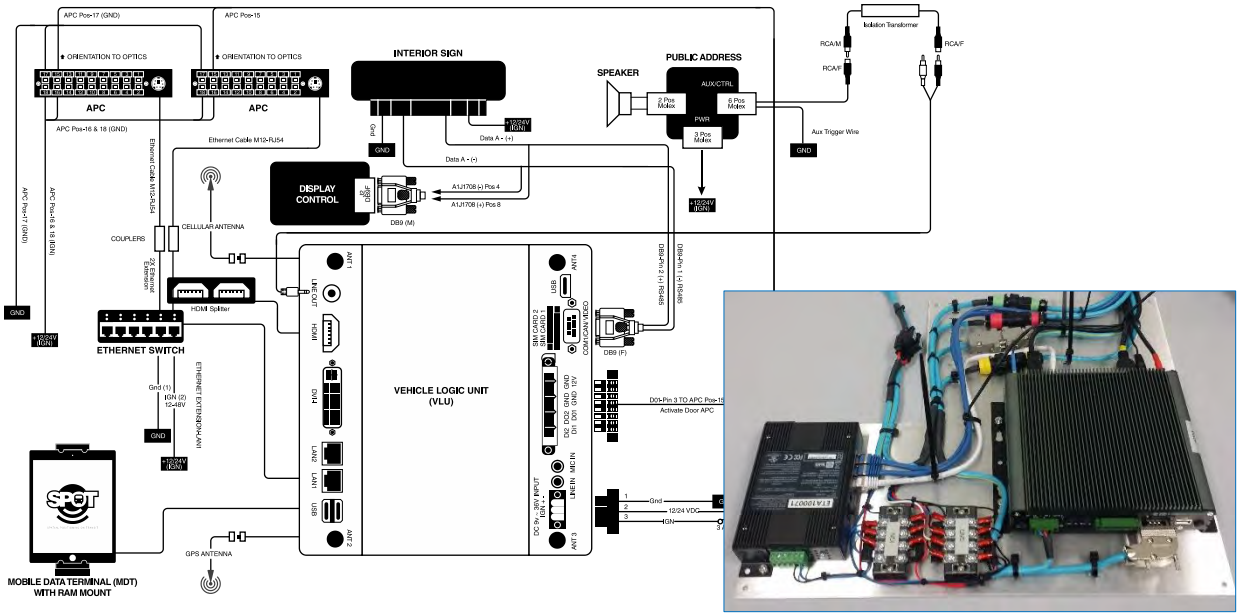


Figure 8: A sample block diagram of a complete SPOT™ ITS installation (left) with wiring harness design (inset).

MDT software

[What you will discover]

SPOT™ provides a customizable and robust suite of administration software that provides GoCOMO an unprecedented level of control over all facets of its operations.

[Section key points]

- **Safety:** Equipped with large buttons, an easy-to-read color scheme, and motion lockout tools, GoCOMO's operators will have the necessary technology to safely perform their job duties
- **Simplicity:** MDTs feature an intuitive user interface with high contrast and modern design to simplify navigation and provide quick access to desired functionalities for GoCOMO's operators
- **Frequent Updates:** SPOT™ is a software as a Service (SaaS) which will ensure the City of Columbia's fleet will always be up to date with the latest technology offered by ETA Transit
- **Electronic Passenger Counter:** The Electronic Passenger Counter (EPC) is a standard component that enables GoCOMO to capture passenger data and visualize it across multiple reports in real-time and can be used for NTD ride checks and APC validation purposes

Let's log in and see what you can do!

When all solutions are comparable, transit agencies report that the overall user experience is most often the deciding factor when selecting a new ITS.

— 2020 ETA Transit Agency Survey

SPOT™ mobile data terminal software

GoCOMO's mobile data terminals include an essential suite of powerful standard software modules designed to simplify daily driver tasks and tools designed to improve the collection of data. By default, MDTs include the following utilities:

- Login module
- Route Selection *or* Set Service module
- Driver Messaging module
- Electronic Passenger Counting module
- Fare Category module
- System Status module
- Anti-Bunching *or* On-Time Performance safety screen

An intuitive user experience

The MDT features a high-contrast modern user interface (UI) designed to simplify navigation and allows drivers to access desired functionalities quickly. The UI of the MDT not only delivers access to software modules, but also provides indicators for new message arrival, system connectivity, time, driver IT, and a one-touch logout button.

Figure 9: The MDT main menu provides the driver with easy one-touch access to all installed software modules.

Driver Login module

Register the vehicle on the SPOT™ platform

Stakeholders impacted: *Dispatchers, Operators*

Upon starting a vehicle, the MDT will prompt the driver to enter the driver ID number **1** and the current odometer **2** reading for the vehicle. The operator will use the numbered keypad on the right of the screen to input the information before tapping the green Login **3** button to commit the details and access the main menu. A successful login to the SPOT™ system kicks off single sign-on process whereupon all connected systems are activated and correlated to the driver's activities for the shift.

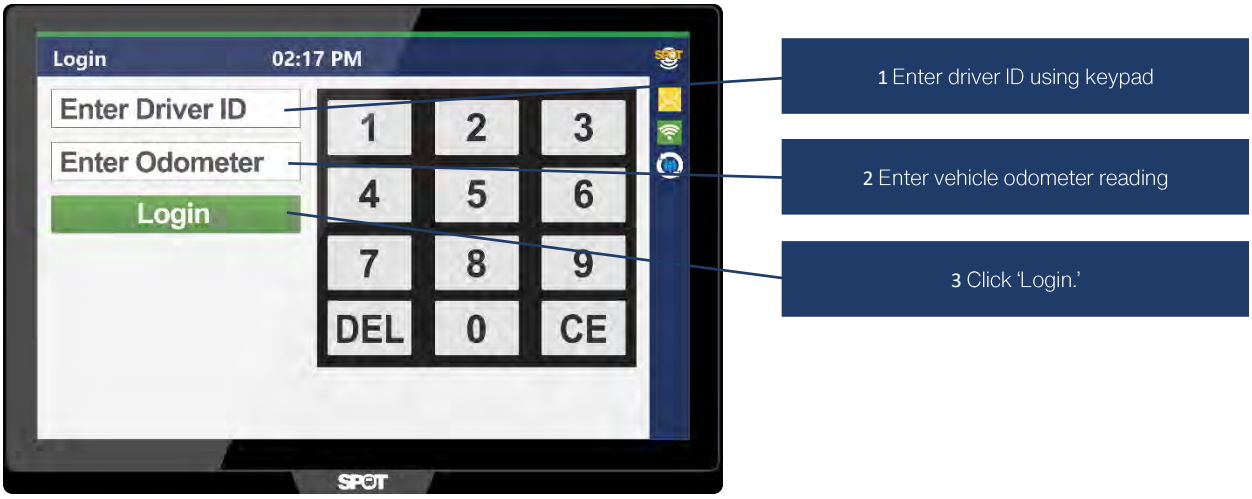


Figure 10: A successful login dictates which software modules are available to an operator and registers the vehicle on the SPOT™ system.

Key concept!

The driver login process is an essential part of collecting both vehicle and route information. Without logging in, the vehicle is untraceable on the system, which impacts data collection, driver behavior monitoring, the calculations of real-time arrival predictions, and the appearance of the asset on traveler information websites and apps.

Set Route/Set Service module

Register the vehicle to a service or route

Stakeholders impacted: *Dispatchers, Operators, Riders*

The Set Route and Set Service modules alert the SPOT™ system that a vehicle is ready to be tracked in real-time, and up-to-the-second ETAs deliver to both the transit agency and its passengers. The operator selects the appropriate option from a list of available routes by tapping on the MDT screen.

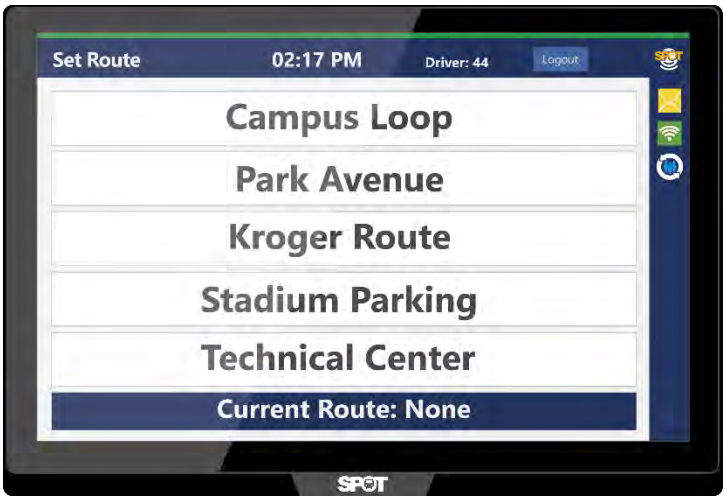


Figure 11: The Set Route module is available on systems running headways.

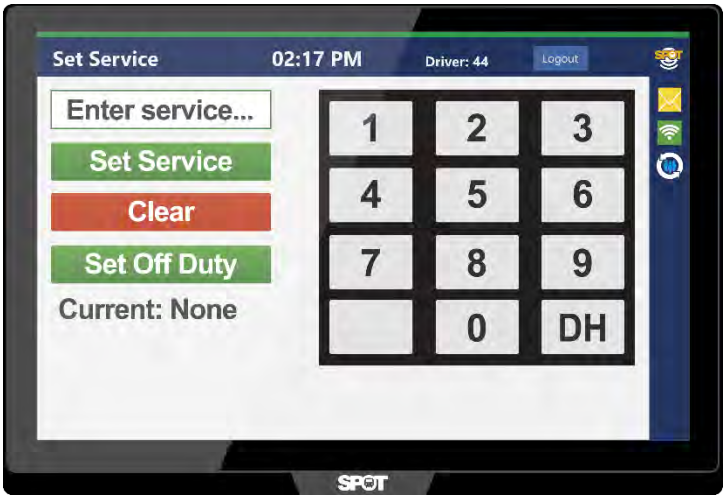


Figure 12: The Set Service module is the standard screen for vehicles running fixed route systems.

Fare Category module

Record passenger boardings by classification

Stakeholders impacted: *Dispatchers, Operators, Riders*

The fare category module provides drivers a simple means of logging passenger type and means of fare uses, including adult, child, senior, and handicap, as well as tracking available capacity for bicycle and wheelchair racks.

Figure 13: Easily log fares and track wheelchair or bicycle storage.

Helpful hint!

The fare categories available in this module are customized by using the Administration>System Configuration>Asset Config tab located in the SPOT™ Administration Console.

Driver Messaging module

Two-way communication between drivers and dispatch

Stakeholders impacted: *Dispatchers, Operators*

Easily communicate with drivers and keep radio frequencies clear with SPOT's two-way Driver Messaging module. Designed to minimize driver distraction, the MDT connects to the administration Driver Messaging module to provide consistent replies and an audited trail of confirmations.

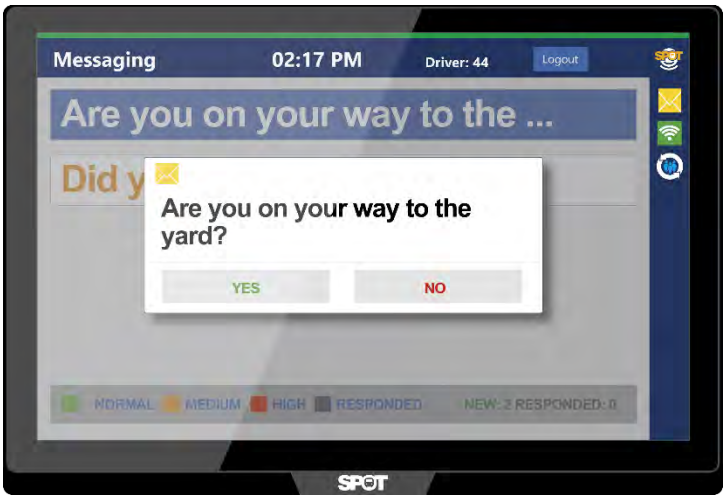


Figure 14: Simple, one-touch confirmations keep driver attention focused on his/her primary responsibilities.

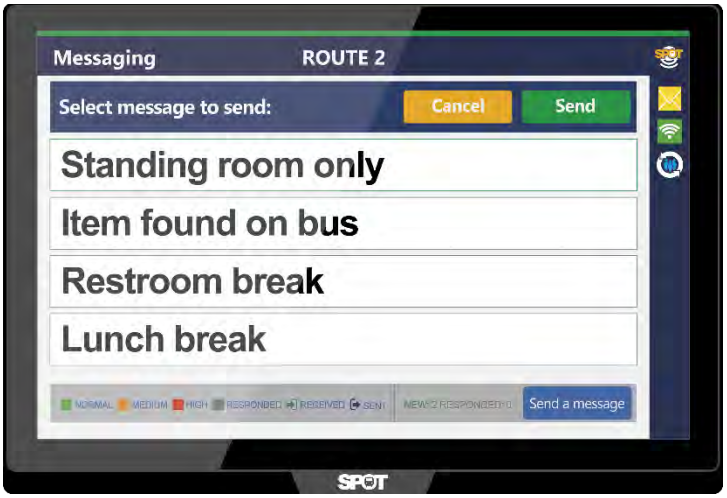


Figure 15: Drivers choose from a pre-defined list of messages to communicate with dispatch. The list of messages is customized during the deployment period to satisfy specific operating requirements.

Electronic Passenger Counting (EPC) module

Accurately record rider boardings and alightings

Stakeholders impacted: *Administrators, Dispatchers, Operators, Riders*

Scrap the clipboard, eliminate manual tallies, and improve counting processes with the Electronic Passenger Counting (EPC) module. Tracking boardings and alightings with tap-tap simplicity. Counts, times, and locations are automatically logged and transmitted to SPOT™ servers for instant access.

Figure 16: The standard EPC module provides an instant upgrade over manual passenger count procedures.

Helpful hint!

Made an error in counting passengers at a stop? Use the (+) of (–) keys to make final adjustments before hitting the 'Send' button.

System Status module

Test your vehicle's connection to the SPOT™ system

Stakeholders impacted: *Operators, Maintenance*

The System Status module provides the first-step solution for identifying onboard connectivity concerns. This handy utility also includes signal strength information and the current GPS location.

Figure 17: The System Status module provides information that can be useful in identifying connectivity issues.

Diagnostics module

A suite of tools to identify potential hardware issues

Stakeholders impacted: *Operators, Maintenance*

An MDT based solution to test connected systems as part of pre-trip inspection and deliver critical information to support and maintenance teams for troubleshooting potential issues.

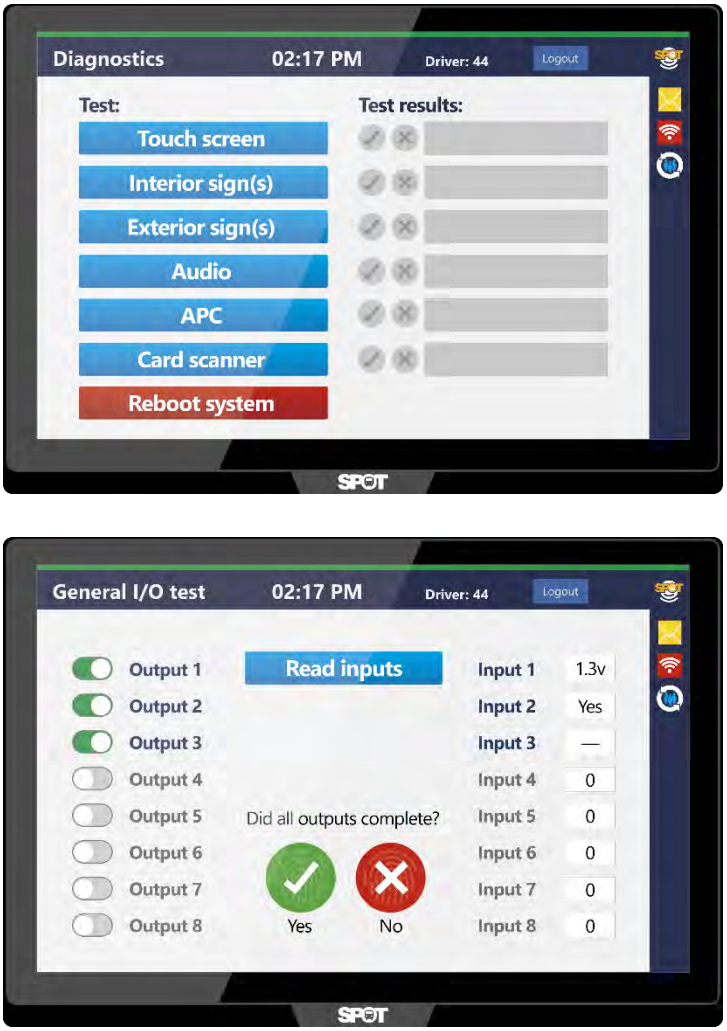
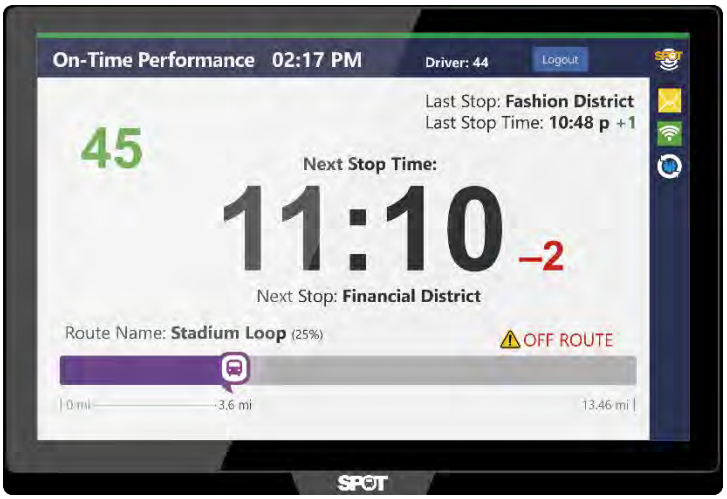


Figure 18: The Diagnostics module contains six essential tools to test connections to onboard hardware.

On-Time Performance lock screen
Real-time status updates for the driver

Stakeholders impacted: *Dispatchers, Operators*

Drivers receive real-time updates of their progress and timing on their assigned route, allowing for intuitive adjustments to stay on schedule.



Anti-Bunching lock screen
Manage spacing between vehicles

Stakeholders impacted: *Dispatchers, Operators*

Maintain ideal vehicle spacing with SPOT's color-coded Anti-Bunching lock screen, which displays a vehicle's current position relative to the assets in front and behind.

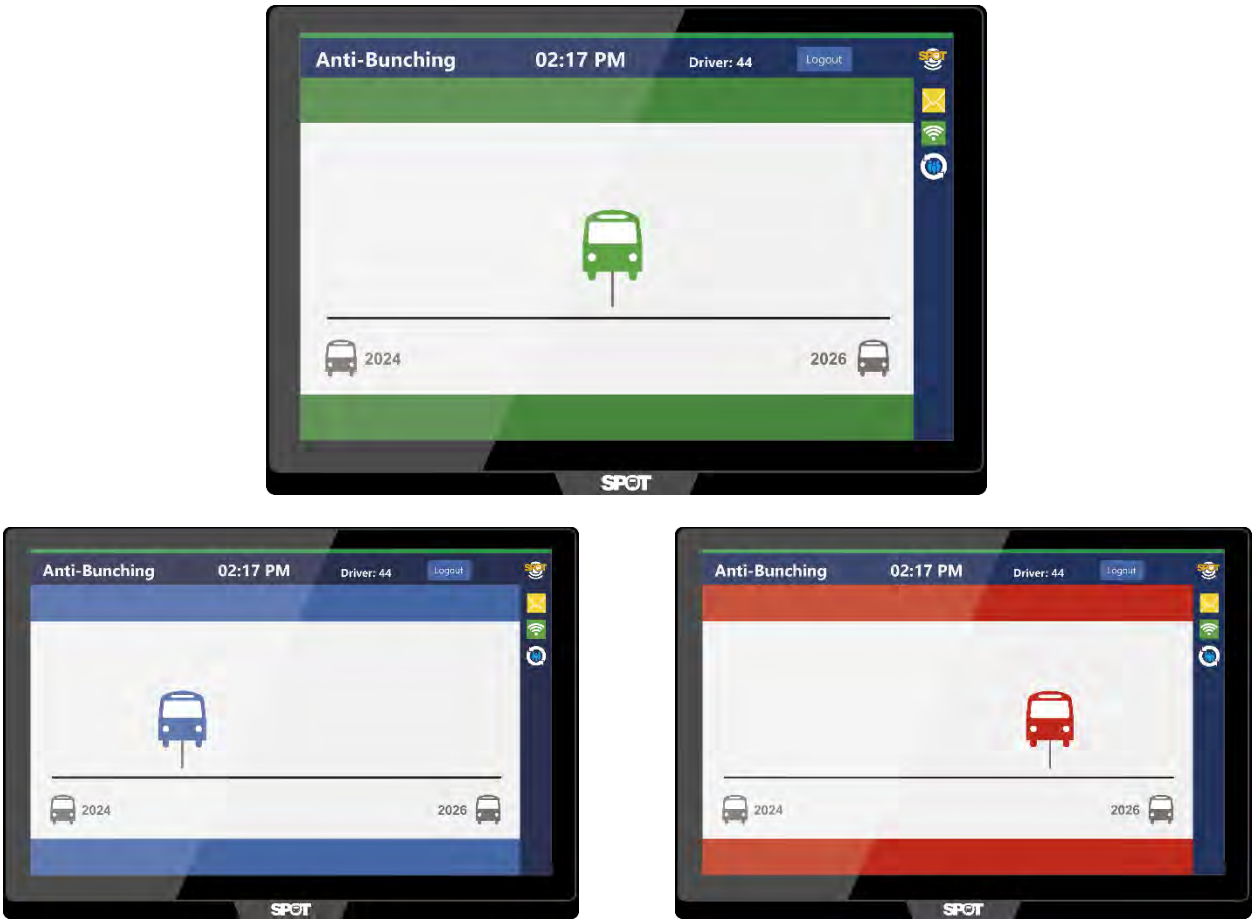


Figure 19: Vehicle position and spacing display in easy-to-understand color codes. Green represents the optimal spacing between assets on the same route; blue indicates a driver is too far away from the vehicle in front, and red shows the bus/shuttle is too close to the one in front.

Back office systems

[What you will discover]

SPOT™ offers an extensive range of software modules designed to enhance GoComo's operational prowess, enhance interaction with your ridership, and efficiently deliver real-time information.

[Section key points]

- **Route Manager:** The Route Manager tool is an advanced GTFS editor that offers extensive capabilities. It empowers GoCOMO to efficiently manage their GTFS data, enabling swift creation of detours, seamless schedule updates, and effective implementation of future operational changes. Moreover, GoCOMO gains full control over managing audio, head signs, and service modifications, eliminating the need to rely on external resources such as ETA for these tasks. With the Route Manager, the City of Columbia can exercise complete authority over their transportation operations
- **100% Web-Based**: The SPOT™ console being a SaSS platform, requires no installation or maintenance of software, allowing users of GoCOMO to access it from any web-browser supported device
- **AVL**: The dispatch module offers full functionality for controlling, communicating, visualizing, and monitoring GoCOMO's fleet, provides the dispatch team with all the necessary tools to maintain situational awareness and the flexibility to make operational adjustments as needed
- **Arrival Predictions**: The back office system, refined over 20 years, provides the City of Columbia with cutting-edge technology to communicate up-to-the-minute arrival predictions to students, faculty, and staff from a single, trustworthy source
- **Reader Boards**: By leveraging either GTFS-RT or SPOT's API, GoCOMO can seamlessly integrate with both existing and new signage systems, thus ensuring a communication system that is future-proof

Let's log in and see what you can do!

Administrators are the leading drivers of change within a transit organization.

— 2020 ETA Transit Agency Survey

SPOT™ administration console

The SPOT™ administration console provides transit dispatchers and administrators with a powerful suite of back-office software modules to intuitively manage and improve operations. The console provides a single point of access to the individual software modules which control the system's various features and capabilities.

The administration console is hosted in the cloud and accessed through any modern Internet browser, such as Google® Chrome™ or Apple® Safari™. This configuration provides numerous benefits to transit agencies, including:

- **Lower cost of ownership**
  No expensive servers to maintain or computers to install or upgrade to run the SPOT™ system
- **Anywhere access**
  Log in on any device with an active Internet connection, such as a laptop, tablet, or smartphone and access your SPOT™ system in real-time, including route management, reporting, tracking, and more
- **Always current software**
  Your back-office systems will feature the latest software versions and capabilities; no need to run upgrades or patches

Figure 20: Access the SPOT™ administration console from any Internet-connected device.

A small step for transit technology, one giant leap for operational awareness.

Out of the box, the SPOT™ platform delivers all the essential tools needed to launch your operations to a whole new level. Included as part of the back-office system are:

- Real-time GPS location updates
- Fixed-route dispatch
- Transit service scheduling
- Route management
- Reporting
- User management

SPOT's core back-office system includes the following standard software modules:

- Driver messaging
- Instant replay
- Map (AVL)
- Reports
- Route planner
- Route manager
- Service messages
- Station manager
- System configuration
- User manager
- View schedules

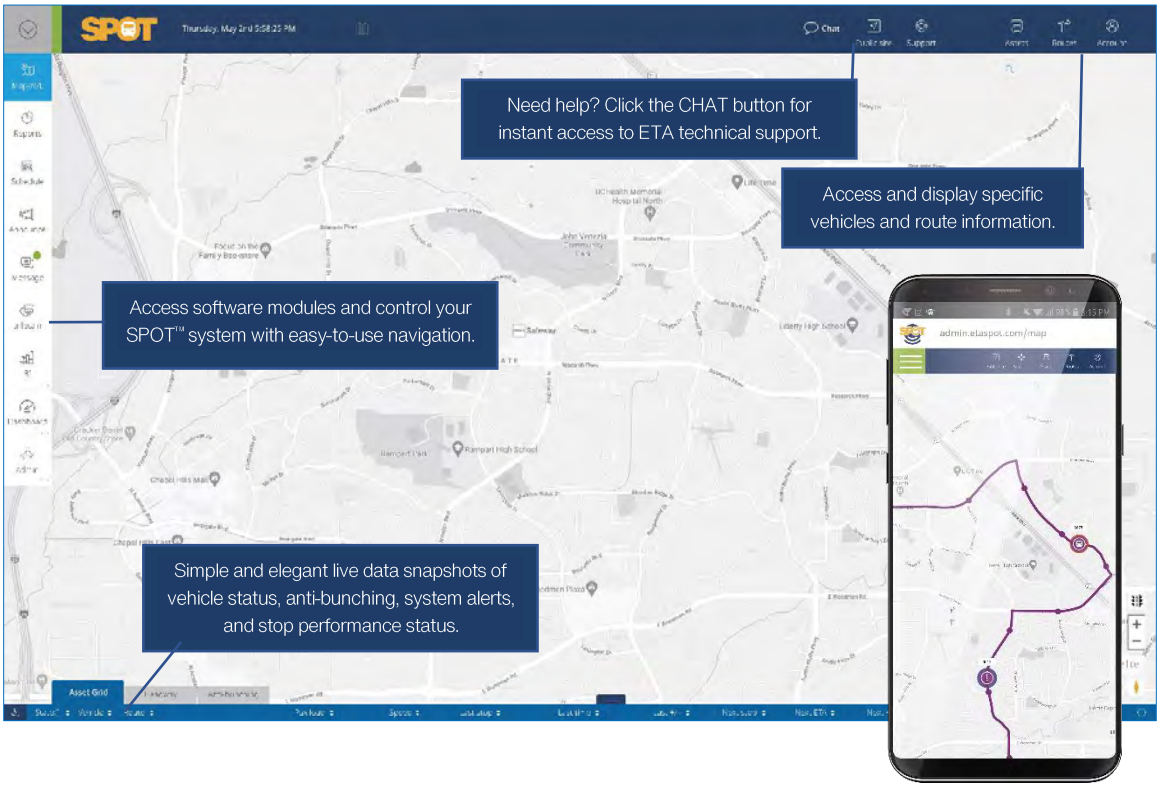


Figure 21: An intuitive interface places all system modules to the left; assets, routes, and chat are located on top; and the bottom of the screen features a tabbed information dock with real-time snapshots of your operational status. This same information is also available on connected smartphones (inset) and tablets.

Route Manager module

Create, control, and edit every aspect of your service

Stakeholders impacted: *Administrators, Dispatchers, Planners*

The SPOT™ Route Manager (RM) delivers an unprecedented level of control to the City of Columbia's services. The RM's capabilities go far beyond drawing a line on a map. It connects your onboard announcements, creates detours, manages Infotainment playlists and triggers, imports, edits, and exports GTFS and GTFS-RT data, and other functions that are associated with services and plans. The whole system places a premium on ease of operation with point-and-click simplicity. Stations, vehicles, media files, and multiple languages are all selectable and coordinated within this intuitive module.

A version-controlled system

The Route Manager is a version-controlled system. It provides system administrators and planners the ability to develop multiple iterations of a plan. It helps create temporary detours and schedules them for a future deployment, and then automatically return to the original plan at the desired date. It manages routes on-the-fly to account for accidents, traffic, emergencies, and other spur-of-the-moment events.

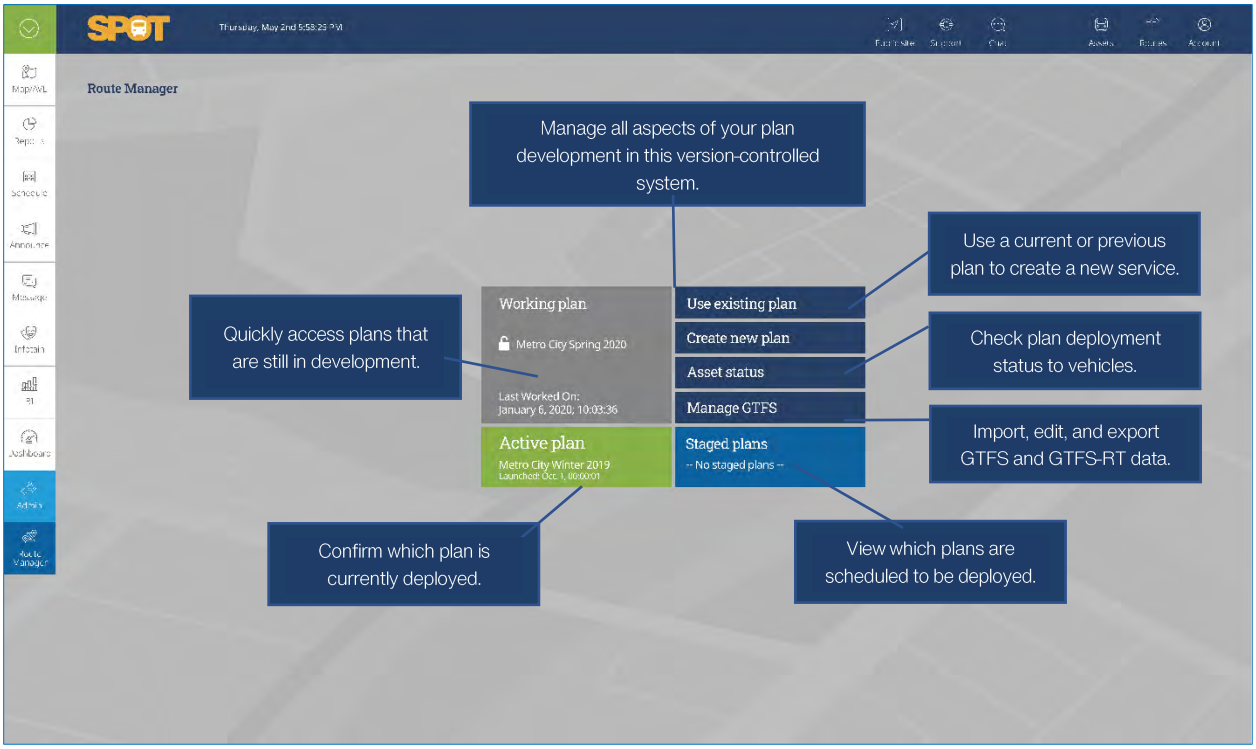


Figure 22: The Route Manager home screen provides a quick launch point for a variety of plan-related tasks.

Notable features and capabilities:

- Create new routes from scratch in minutes with drag-and-drop simplicity
- Create temporary detours
- Publish new plans with a click of a button
- Import, export, and edit your GTFS and GTFS-R data
- View the publish status of existing plans
- Create and stage multiple route plans and have them automatically deploy based on a schedule you define—days, weeks, or months in advance
- Assign vehicles to routes based on short- or long-term needs
- Built-in support for multimodal transit agencies who run both buses and trains
- Create custom geofences and define enter/exit triggers
- Create onboard announcement using audio files or text-to-speech options
- Upload and configure audio announcements to play based on a route, stop arrival or departure, and adjoin other announcements
- Create custom leg actions and pattern selection
- Built-in multi-language announcement support including English, Spanish, French, and more
- Change destination sign codes
- Auto-generate timetables with custom trip start/stop times and frequencies

Route and plan creation:

Route creation in SPOT™ is point-and-click simple, and paths automatically snap to roadways based on direction. Easily name patterns, edit shapes, define specific locations (stops) and trigger points (geofences), manage timetables, enter farebox IDs, create blocks, and even program audio announcements.

Key concept!

An essential idea that defines the behavior of the Route Manager is to imagine that every component assigned to a route nest within a container, which provides an increased level of granular control. The deeper one progresses within the creation of a plan; the more options are available to fine-tune the behavior of a route.

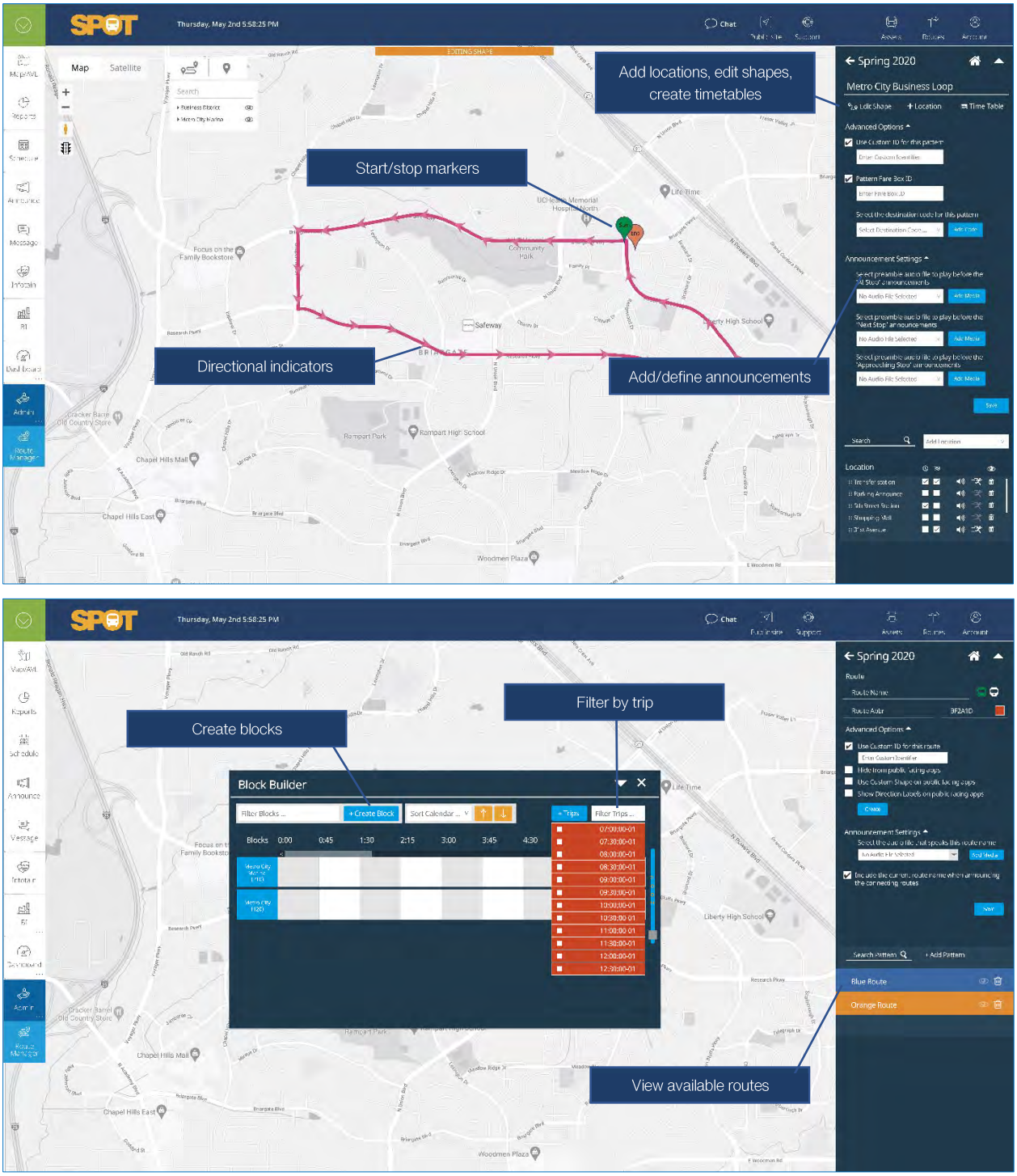


Figure 23: SPOT's Route Manager provides an exceptional amount of control, including on-the-fly detour and route announcement creation. Easily manage leg actions, patterns, destination signs, create blocks, and more.

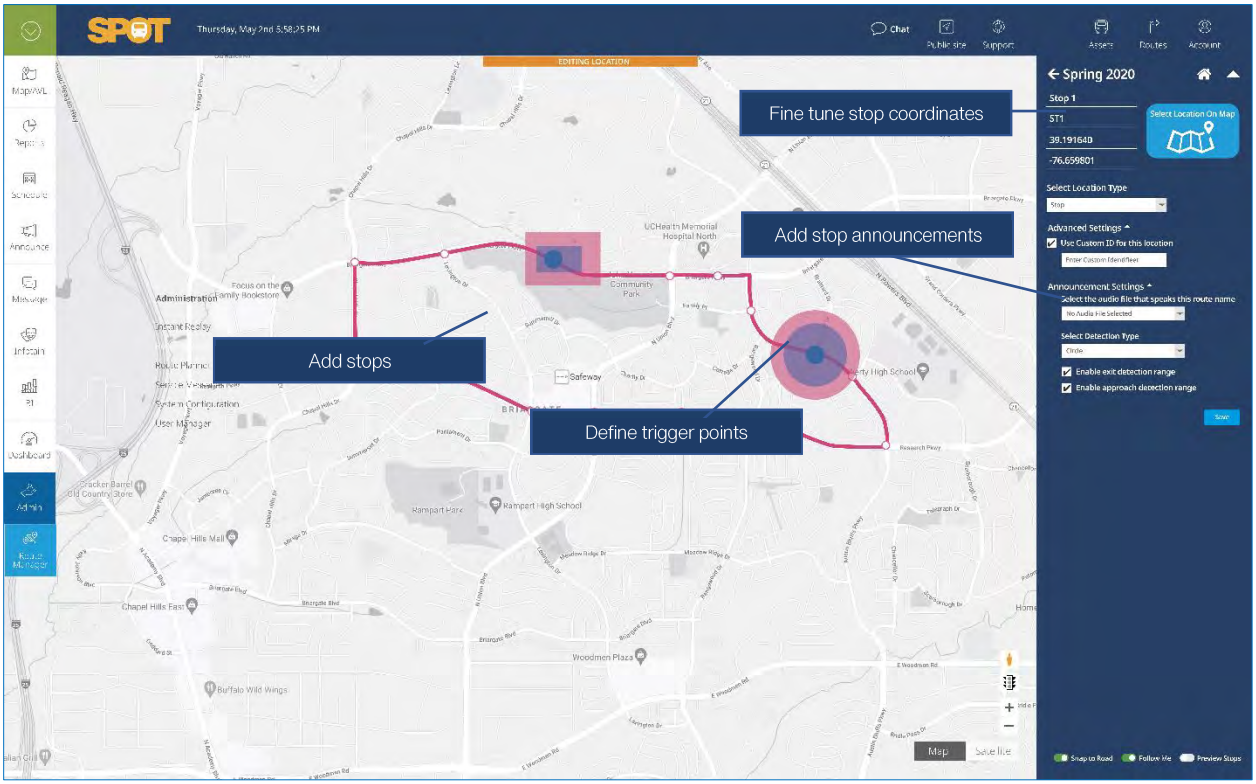


Figure 24: Create finely tuned geofences, custom IDs, locations, and announcement triggers.

Audio and language support

Upload and manage audio route announcements on both macro and micro levels, down to individual stops based on direction, date, time, and location. Multi-language is supported.

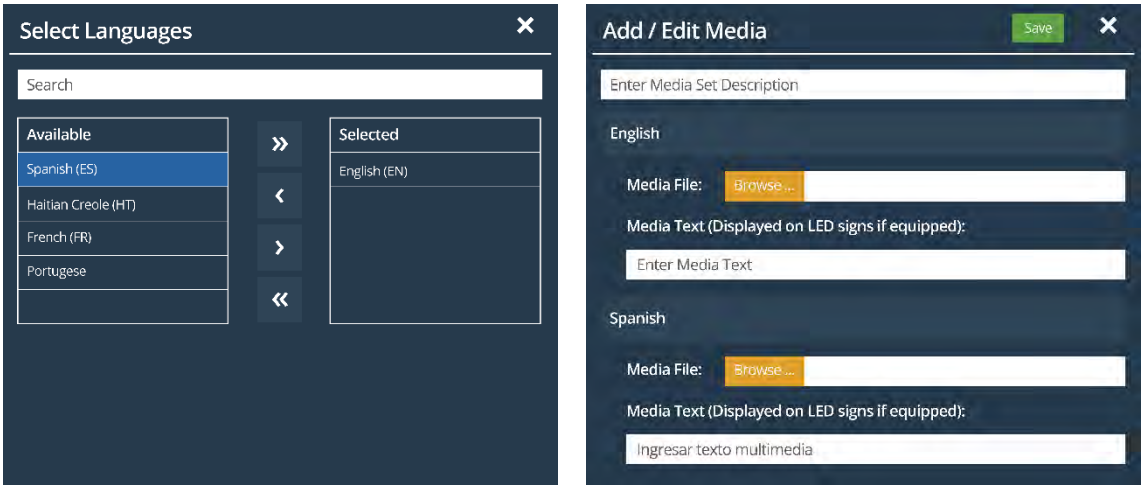


Figure 25: Easily add new language support for announcements (left) and upload audio MP3 files through the media manager (right) in the appropriate section. Add multilingual text for display on connected LED signs.

Working with GTFS data

Import your existing GTFS data, and your routes automatically create within the Route Manager. Edit your GTFS data by making changes to your routes, announcements, and timetables. Once done, export the information to new GTFS files and connected systems automatically update with the new routes, real-time passenger information, alerts, and updates.

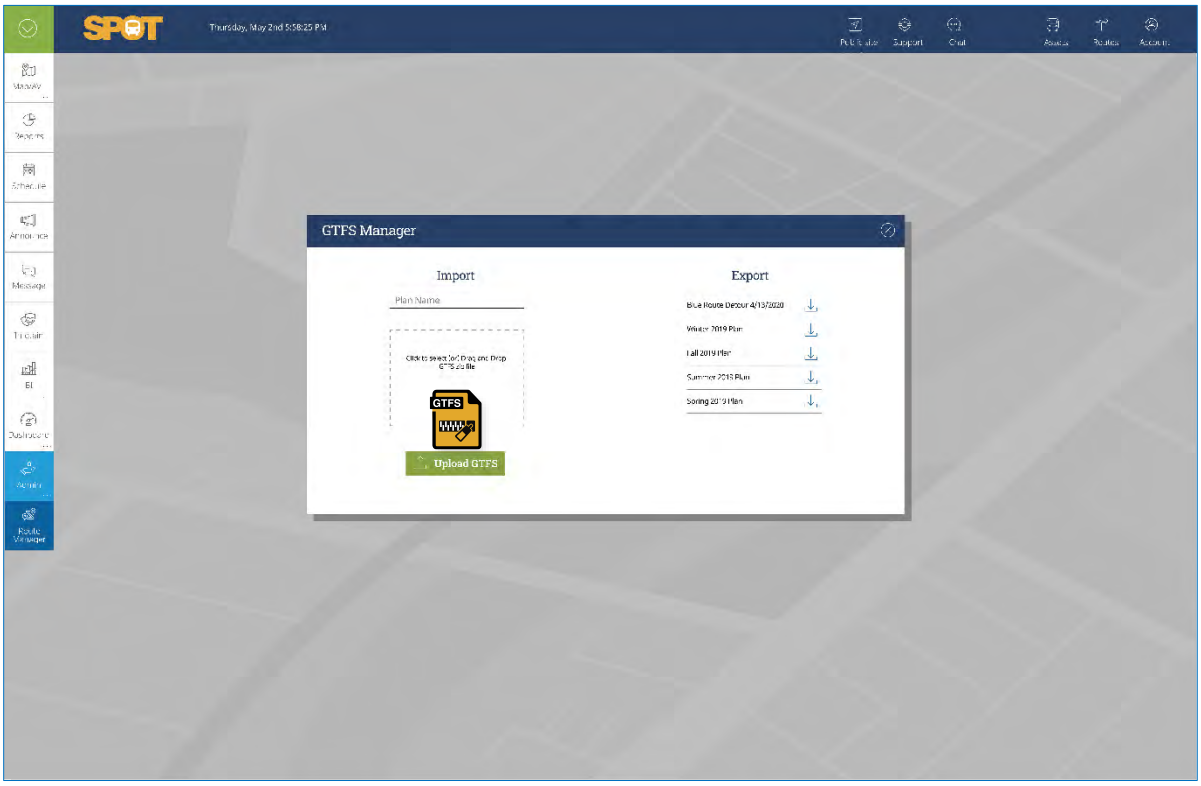


Figure 26: Easily create a new plan based on existing GTFS data. Name the plan, drag GTFS.zip file into the window, click 'Upload GTFS' and let Route Manager do the rest!

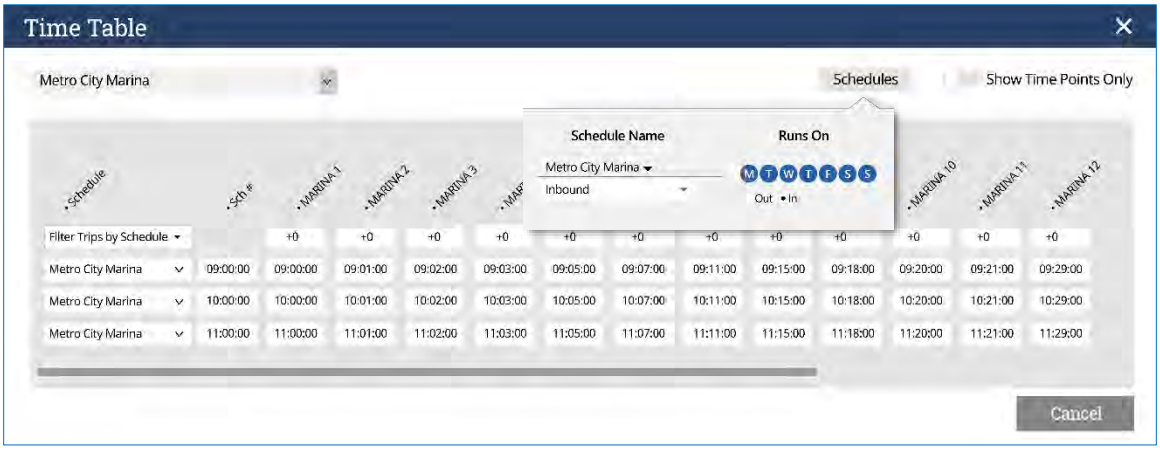


Figure 27: Once GTFS information imports, you can edit routes and timetables, and export the changes to a new GTFS file.

Map (AVL) module
Real-time operational awareness

Stakeholders impacted: *Dispatchers, Road Supervisors*

The Map module delivers real-time operational awareness for transit agencies for both vehicle and stop performance. Dispatchers will benefit significantly from this module as it serves as a front-line utility to:

- Track vehicles by run, route, speed, location, and more
- Monitor on-time performance and real-time passenger loads
- Dispatch vehicles to routes
- View current vehicle spacing
- Last communication times, GPS connectivity, and more
- Configurable asset updates from as little as one second
- Display real-time stop performance

The Map module leverages Google® Maps™ and its familiar set of navigation tools, such as pan and zoom to assist the user with a convenient means of tracking specific vehicles or geographic areas.

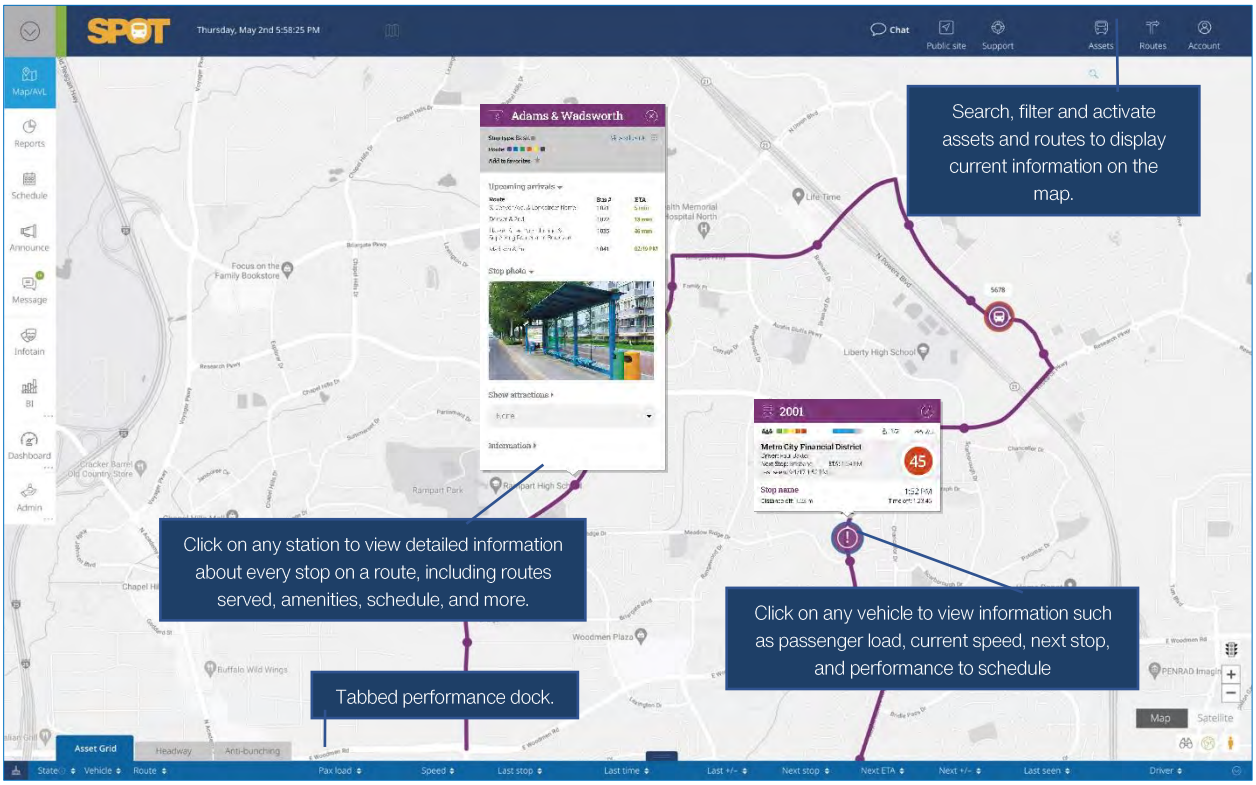
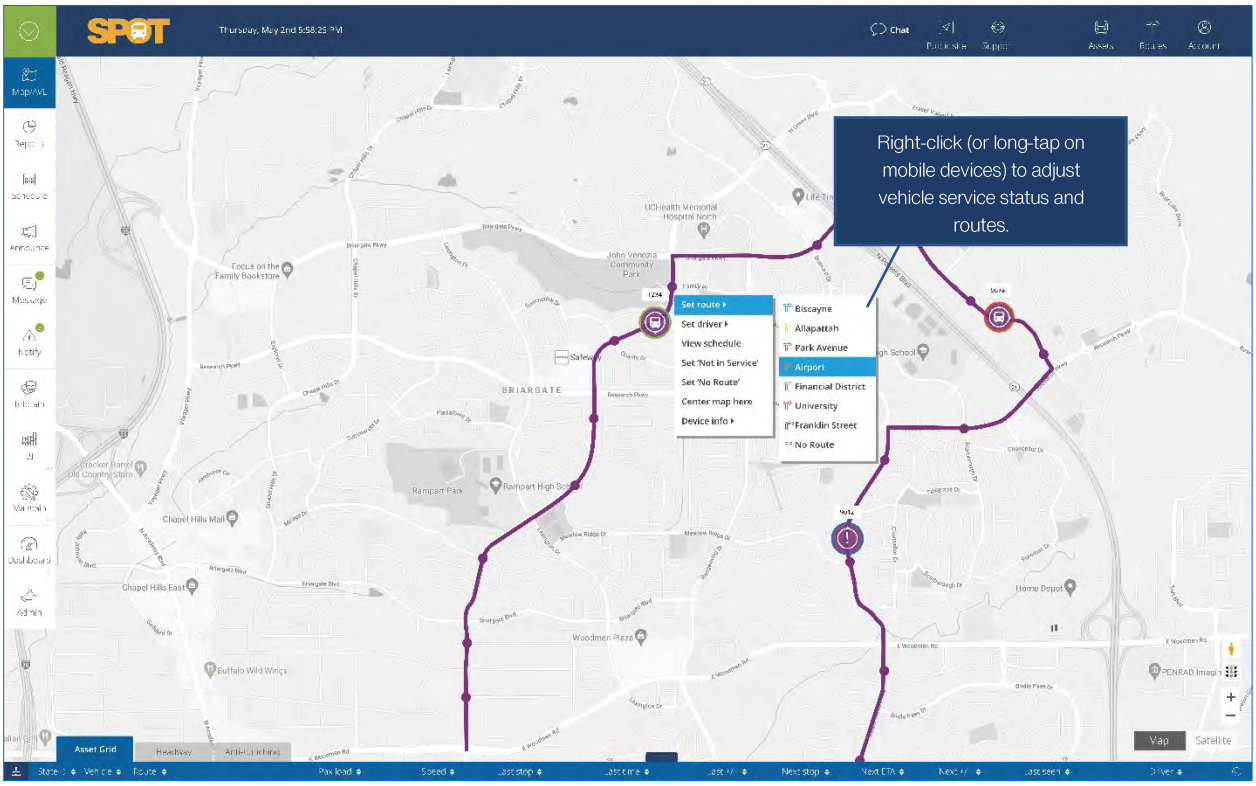


Figure 28: The Map module is the go-to resource for real-time status on any route or asset.

Contextual menus

Right-click on any asset icon to quickly assign the vehicle to a new route, view assigned schedule, set to not in service, set to no route, center the map on the asset, or identify the address of the onboard modem (device info).



Color-coded assets

Assets move smoothly along assigned routes in real-time. Each asset displays as a color-coded icon indicating its performance to schedule (red=late, blue=early, green=on-time). Additional symbolic information is provided for off route, not-in-service, not tracking, and no GPS issues.

Helpful tip!

The icon of any asset contains a wealth of information about the status of the vehicle.

Outer color: Assigned route
Inner color: Schedule performance
Inner icon: Asset status

Vehicle in service
Not in service
Not tracking
Off route
No GPS
Upper level

Tabbed performance dock

At the bottom of the Map module, useful information about the operation displays via a tabbed dock. This dock contains an asset grid, anti-bunching, system alerts, and stop performance views. Each delivers at-a-glance operational information useful for identifying situational concerns. Depending upon GoCOMO and operational configuration necessities, the dock may provide:

Asset Grid: A real-time view of all specified vehicles, on-time performance, passenger counts, speed, last interaction with SPOT™ servers, and last/next stop arrival predictions.

Figure 29: Asset Grid tab.

Headway Performance Tab: Ideal for agencies running headways, the Headway Performance tab monitors stations and logs the time since the last vehicle visit and calculates the next arriving asset.

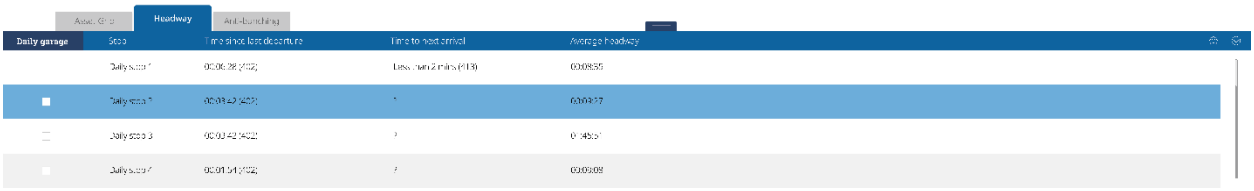


Figure 30: Headway Performance tab.

Anti-Bunching Tab: View the proximity of multiple assets on any route with the vehicles in front and behind to help make spot judgments to ensure optimal spacing and timing between stops. The Anti-Bunching tab displays relative position to assets and stations and utilizes color-coded on-time performance markers.

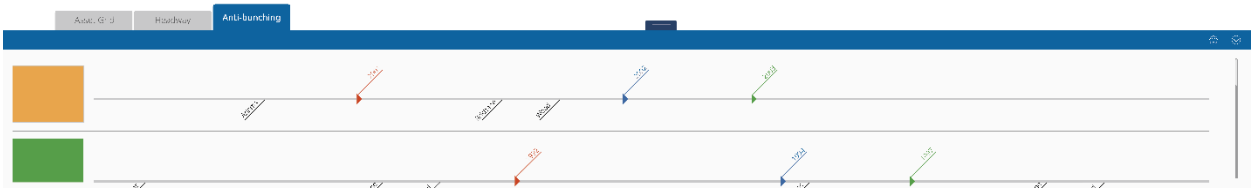


Figure 31: Anti-Bunching tab.

Reports module

Over 100 queries to analyze operational performance

Stakeholders impacted: *Administrators, Dispatchers, Planners, Supervisors, Executives*

Data collection is the beating heart of any intelligent transit system, and SPOT™ provides a robust set of reporting tools to help access this critical information. With over 100+ canned report queries, this module provides you the critical insights into the performance of your transit agency and dramatically simplifies your NTD reporting process.

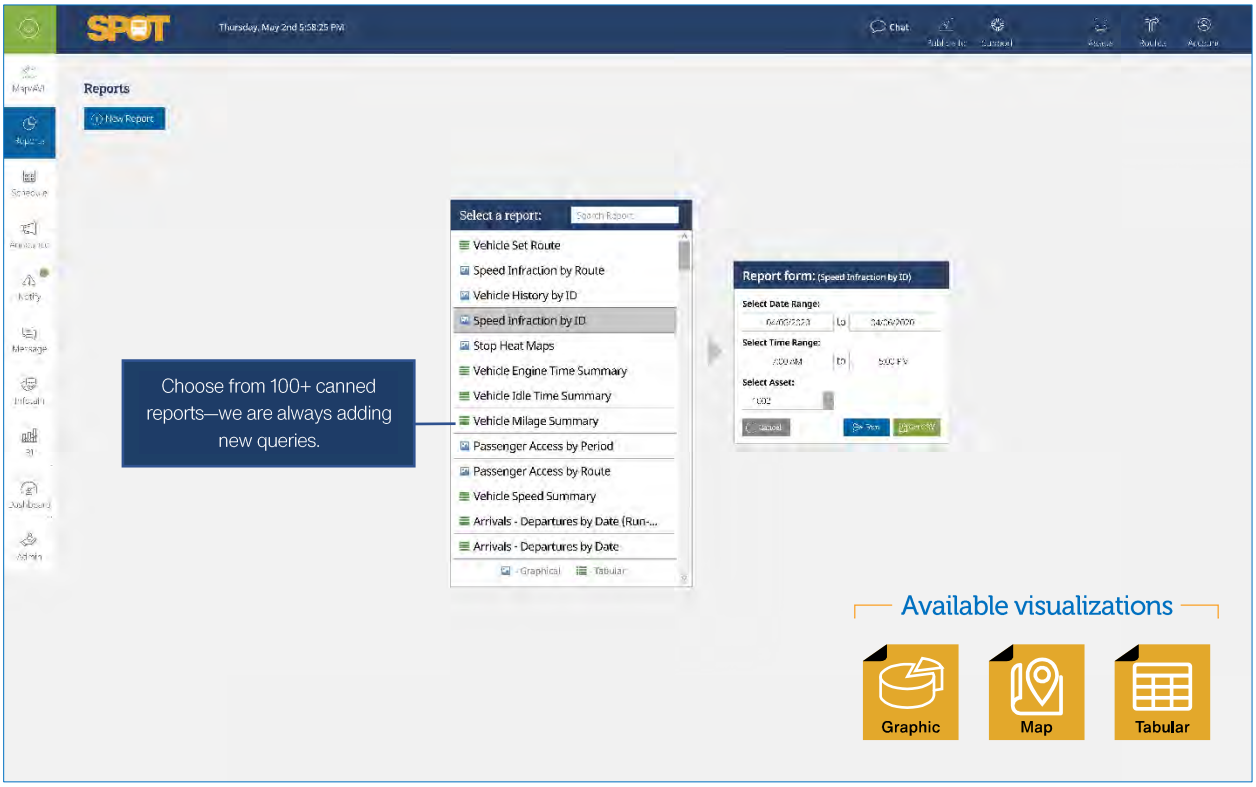


Figure 32: Search for queries by name or scroll through a list of all available reports. Select an area for analysis, click 'run,' and your requested data arrives within seconds.

The Reports module features must-have analysis* of:

- Passenger counts
- Ridership by type, route
- Unlinked passenger trips
- Fare counts by station or vehicle
- Hours/mileage by vehicle
- Vehicle engine summary time
- On-time performance
- Speed infraction by ID
- NTD reports

** - See a full list of available reports in Appendix A: Report listing*

Essential features of the Reports module include:

- Data export to CSV
- Filtering
- Printing of selected information
- Lifetime access to all data from day one

Tabbed reporting

With SPOT's tabbed reporting feature, viewing multiple reports in a single window streamlines your data review process. Easily switch between tabs to compare results, or re-run queries in the same space. The report module window makes it easy to output results to a printer or spreadsheet (via CSV format) for further analysis.

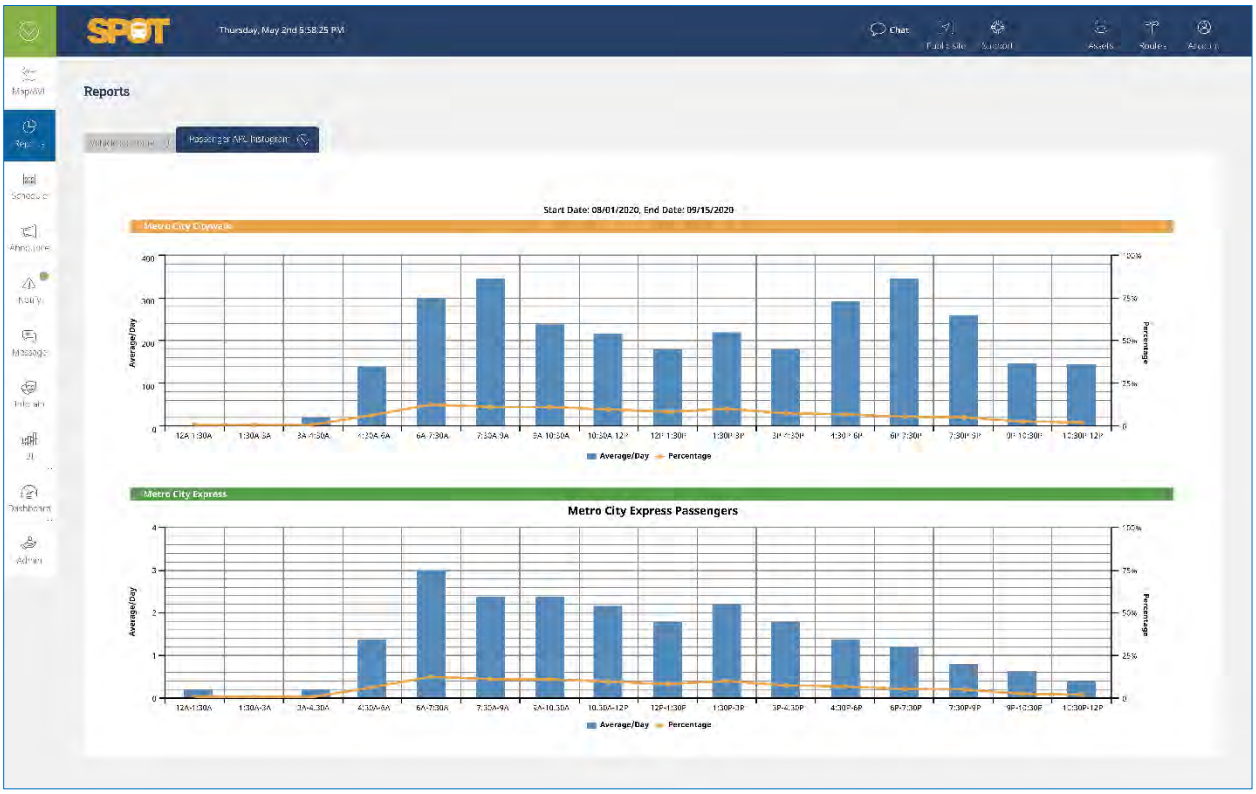


Figure 33: Sample graphical report.

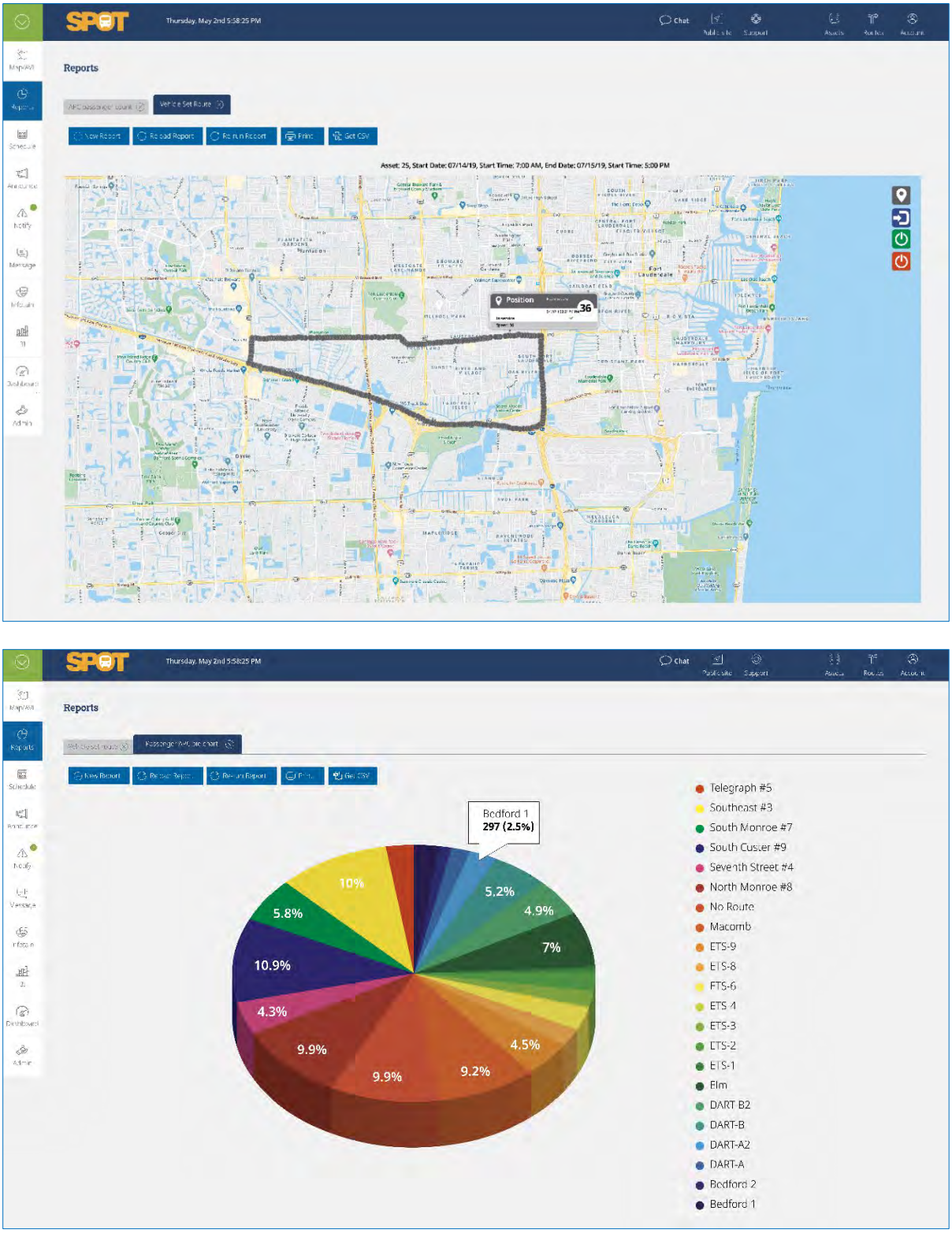


Figure 34: Sample map-based breadcrumb (top) and graphical charts (bottom) reports.

Weekly Google Analytics reports

Each week, ETA sends GTA a Google® Analytics™ report that tracks the use of the public site to provide insights into how riders are utilizing your system. This report includes:

- Total site visitors
- Desktop/tablet/mobile utilization
- Favorite stops
- Favorite vehicles
- Visitor location
- and more...

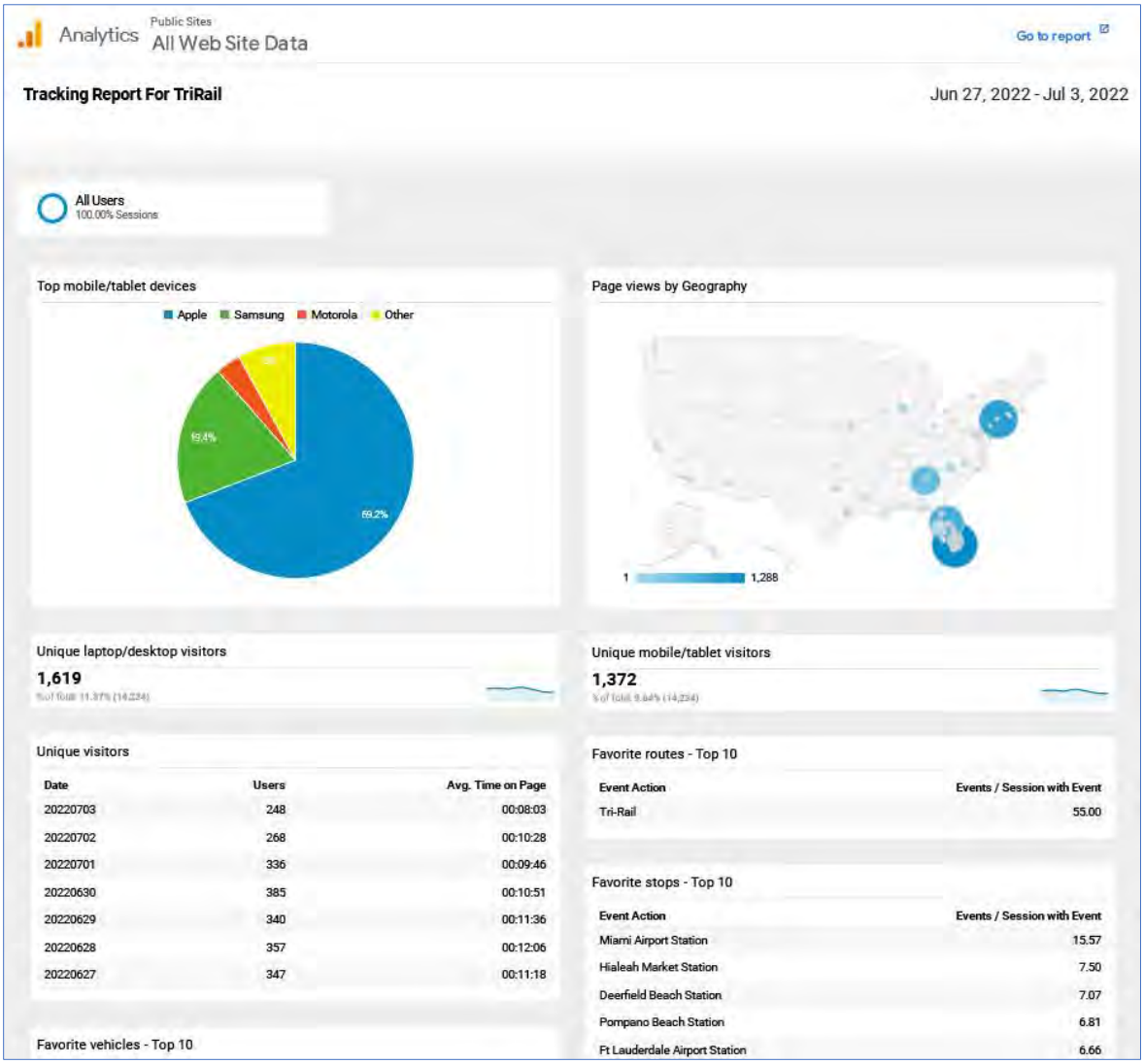


Figure 35: The weekly analytic report delivers high-level insights into how riders use the City of Columbia's services.

Schedules module

Reference schedules quickly with the latest route information

Stakeholders impacted: *Dispatchers, Planners*

The Schedules module is primarily used for fixed-route operations to examine individual bus schedules (by route, weekday, etc.). The module provides a quick and easy reference to your timetable information. Synchronized with your GTFS data, this module is always up to date and can be filtered for quick reference, printed, and exported.

The View Schedules module provides:

- Drop-down schedule selection and one-click filtering
- Easy printing of selected information
- PDF download of schedule information

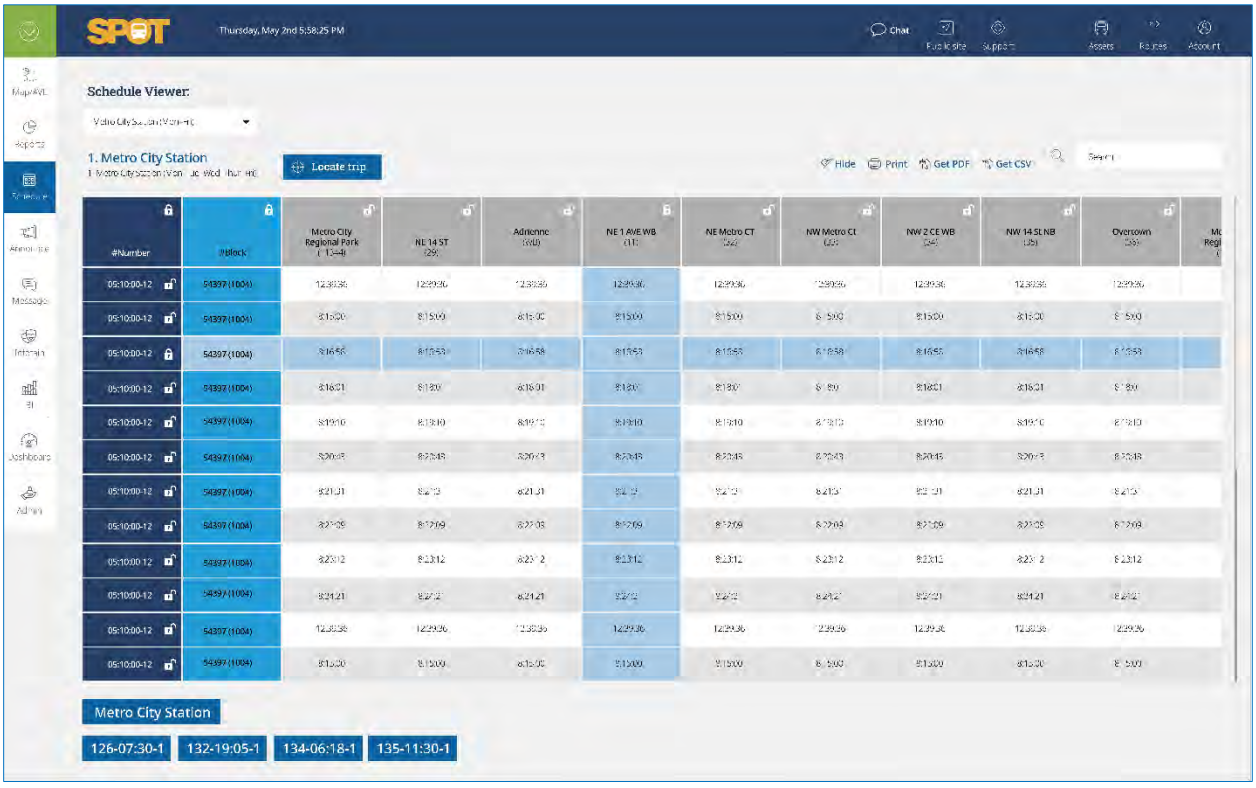


Figure 36: Use the View Schedule module to reference, print, and download route timings.

The information contained in this module can be used to serve multiple purposes, such as providing up-to-date schedules on agency websites, connected passenger information systems, and onboard display signage.

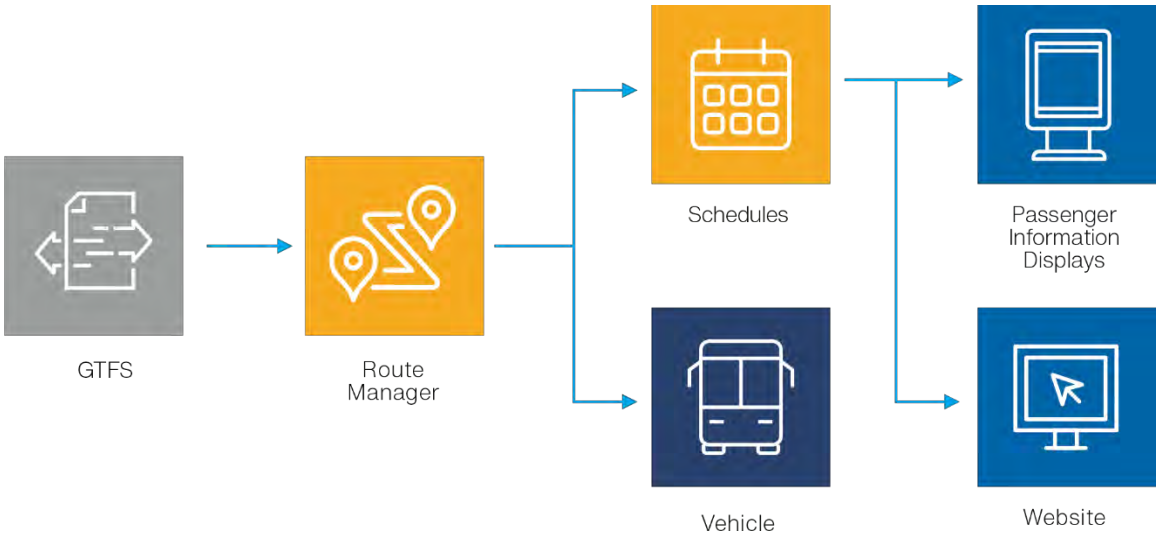


Figure 37: GTFS information is imported into the Route Manager for editing/management. This updated information is then passed to assets and the Schedules module for use in agency websites and connected display systems.

Helpful tip!

Click on any row and select 'hide' to remove the schedule number from view.

Driver Messaging module
Communicate safely with operators

Stakeholders impacted: *Dispatchers, Operators*

The SPOT™ Driver Messaging module establishes a safe, non-intrusive link between dispatch and operators via the vehicle's mobile data terminal (MDT).

Key features found in the Driver Messaging module, include:

- Confirmation and acknowledgment driver response options
- Canned driver messages to dispatch
- Support for auditing and receipt of delivered messages
- Individual vehicle or group messaging capabilities
- Define message priority
- Message auditing, including times of receipt and response and vehicle location

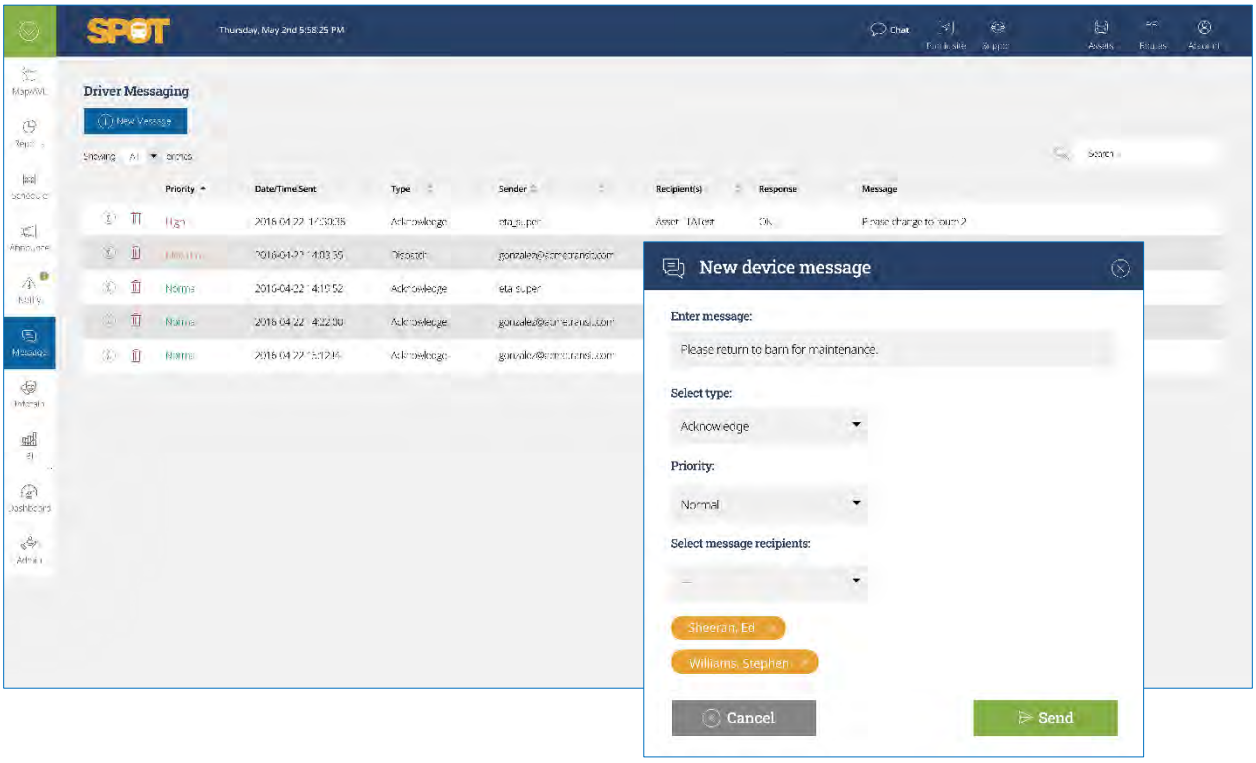


Figure 38: Dispatcher view of the message queue in the administration console (top), and the new message creation dialog (inset).

Dispatch messaging to drivers

A dispatcher will communicate to driver through the Messaging module, a can craft specific messages relative to the need. These text-based communications have two types of reply: acknowledgement or YES/NO. A yellow envelope icon is displayed in the upper right corner of the MDT alerting the driver to view the message at the next available opportunity,

For safety purposes, a driver cannot respond to a question with text response nor while the vehicle is in motion. Incoming messages are color-coded based on priority (red=high, gold=medium, green=normal). Once a message has been read and acknowledged, its color in the queue changes to gray.

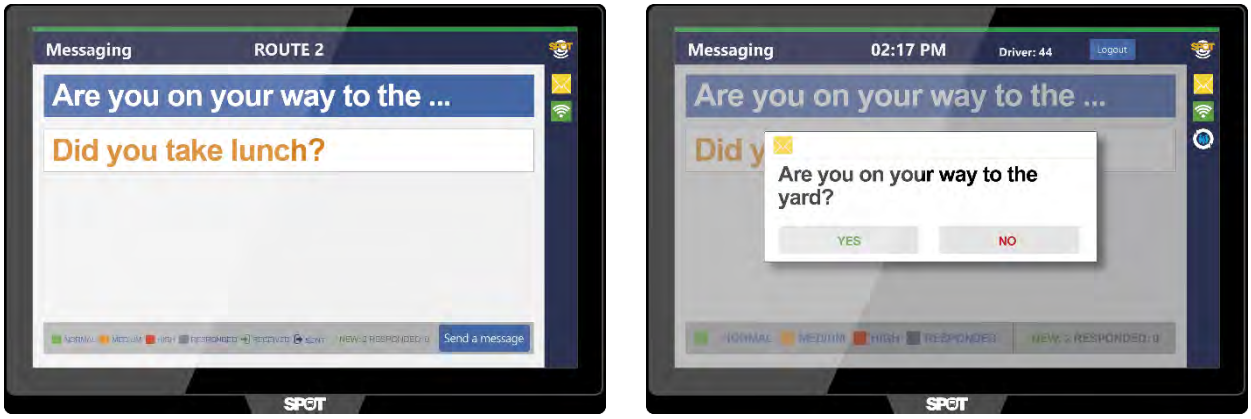


Figure 39: The driver MDT view of the current message queue (left), with a YES/NO response (right).

Driver messaging to dispatch via MDT

The ability to communicate to dispatch is a crucial tool to allow rapid response to non-emergency situations, and the SPOT™ MDT Driver Messaging module provides a quick, efficient solution that keeps drivers focused and dispatchers aware of pending concerns.

The solution comes in the form of canned, agency-defined messages that can be queued up and transmitted with just a couple taps of the mobile data terminal. This list of 'canned' messages can be configured at any time to ensure that common situational responses are covered.

The result is an effective means of two-way communication that reduces background radio chatter and keeps driver eyes on the road.

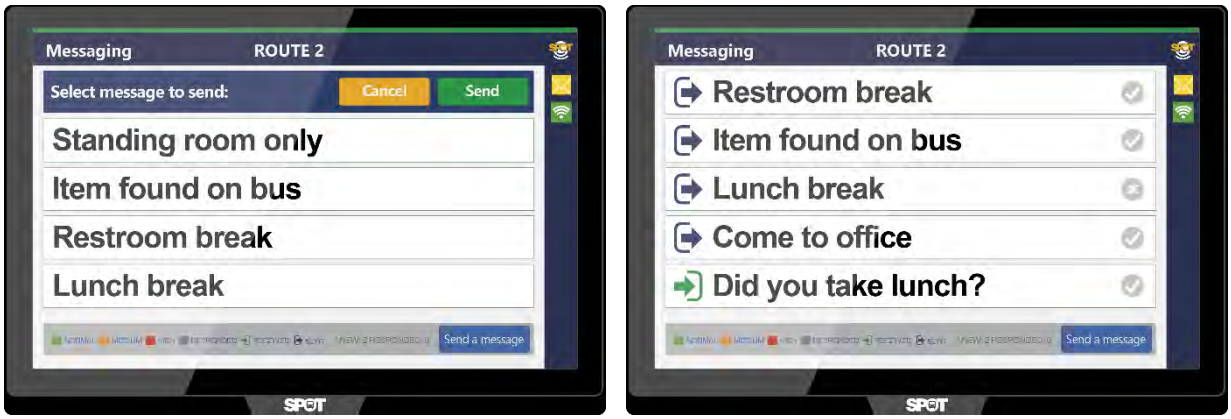


Figure 40: Transit agencies may choose from a list of canned messages for a driver to send to dispatch—or create a custom set to meet specific operational needs (left). All incoming and outgoing messages log in the MDT (right). Operators are notified of pending messages by a yellow envelope icon in the upper right corner of the display.

Helpful tip!

Quickly locate messages in the Driver Messaging console by sorting based on priority, date/time sent, type of response, sender, and more!

Instant Replay module

Rewind and visualize asset performance

Stakeholders impacted: *Administrators, Dispatchers, Operators*

The SPOT™ Instant Replay module provides a data-driven recreation of recorded vehicle information, allowing transit agencies to review the entirety of their operation for both performance and incident evaluation. With this module, agencies can:

- Back up, speed up, slow down the replay speed
- View history by route or vehicle
- Identify instances of speeding, excessive idling, missed stops, passenger counts, and more
- Choose a specific date or time, or select multiple days and time ranges

The module provides an easy-to-use timeline-based interface that should be readily familiar to anyone who has used an online streaming media or DVD player. Users specify the date and time range and then use the controls to play/pause and fast forward.

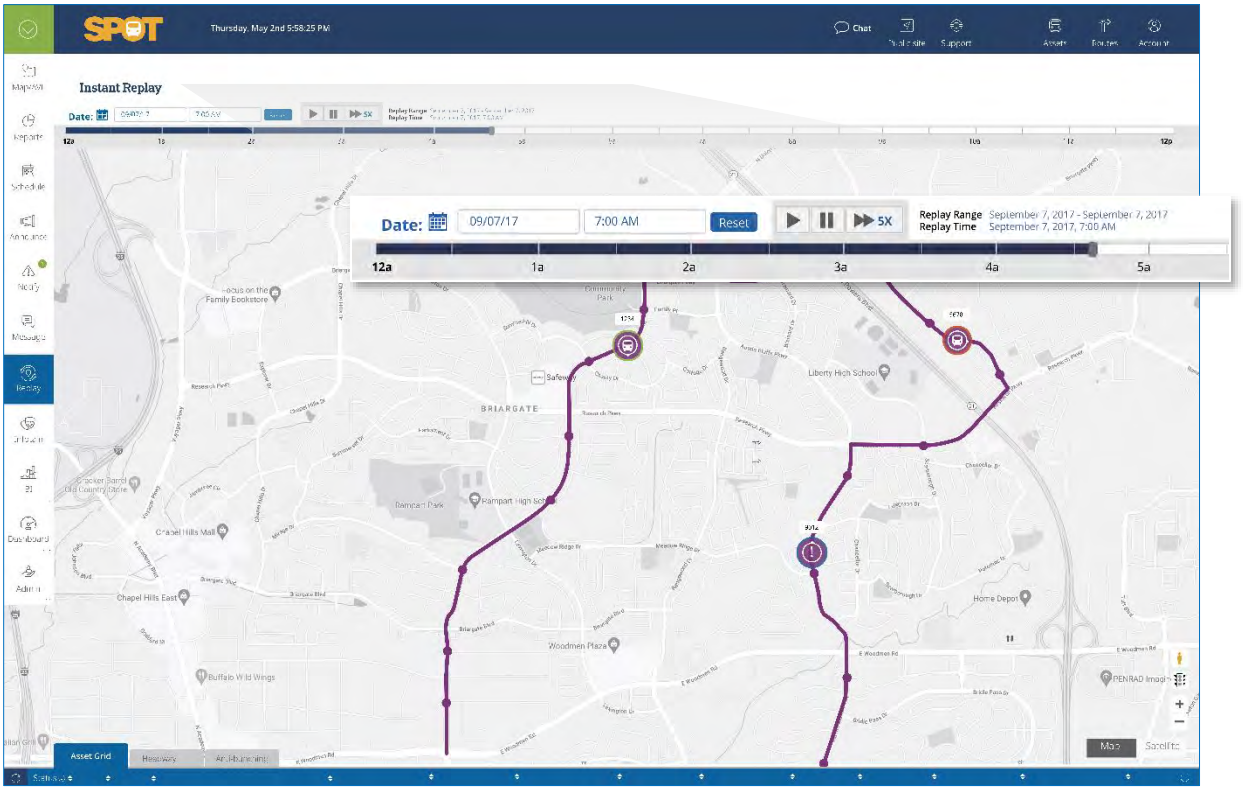


Figure 41: Use the timeline bar to navigate transportation data to identify potential system improvements, asset performance, investigate incidents, and more.

Route Planner module
Assign drivers and vehicles to routes

Stakeholders impacted: *Dispatchers, Operators*

The SPOT™ Route Planner module is a handy tool to perform vehicle assignments and create custom run cuts by adding additional trip legs. By using existing route data, the system automatically attaches a vehicle to the work assignment at the appropriate time and location.

Use the Route Planner to:

- Import vehicle service assignments from existing third-party systems
- Assign vehicles to routes and drivers to vehicles
- Save plans by day, or standardize long-term assignments

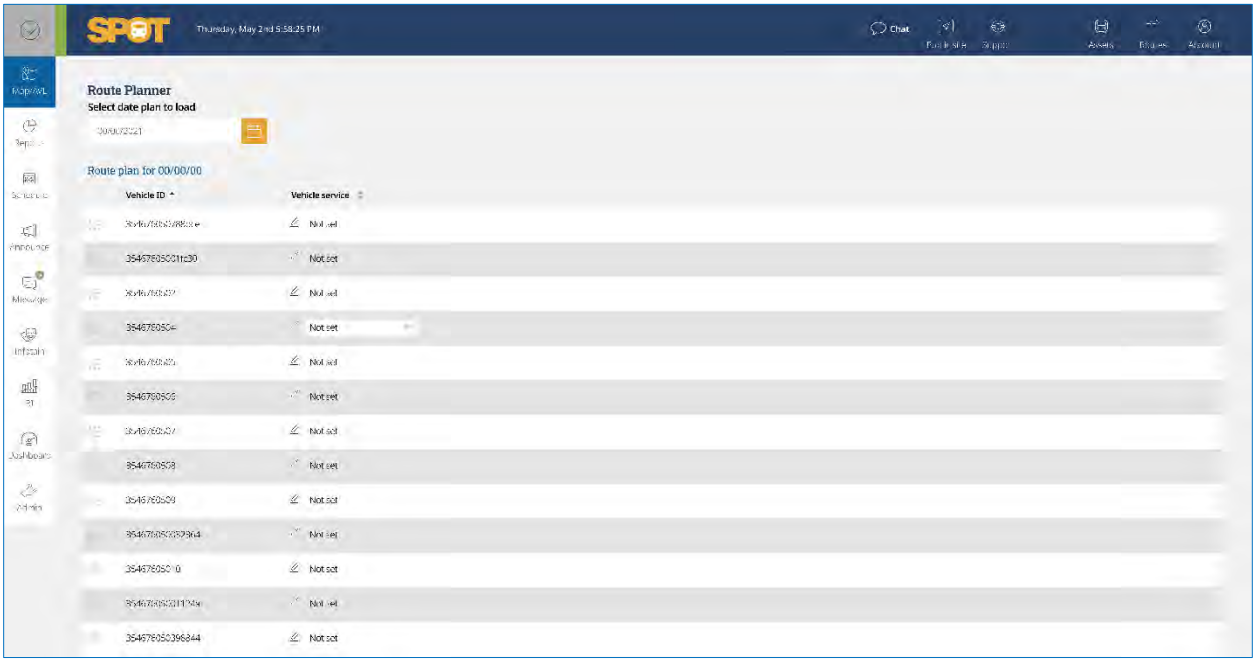


Figure 42: Assign vehicles to drivers and routes with point-and-click simplicity.

Key concept!

Service assignments take effect when a vehicle makes a complete stop at a known stop on an assigned route.

Service Messages module
Communicate with riders in real-time

Stakeholders impacted: *Dispatchers, Operators, Riders*

An informed ridership is a critical component in maintaining a passionate and dedicated customer base, and ETA's Service Message module seamlessly communicates alerts and notifications to all connected websites, signs, stations, and mobile apps in real-time.

Featuring an intuitive interface, administrators and dispatchers will have no difficulty in scheduling system messages for future deployment or whipping out a spur-of-the-moment service alert. The module provides a simple means of managing existing messages, assigning priority, and defining a lifespan for your rider communications.

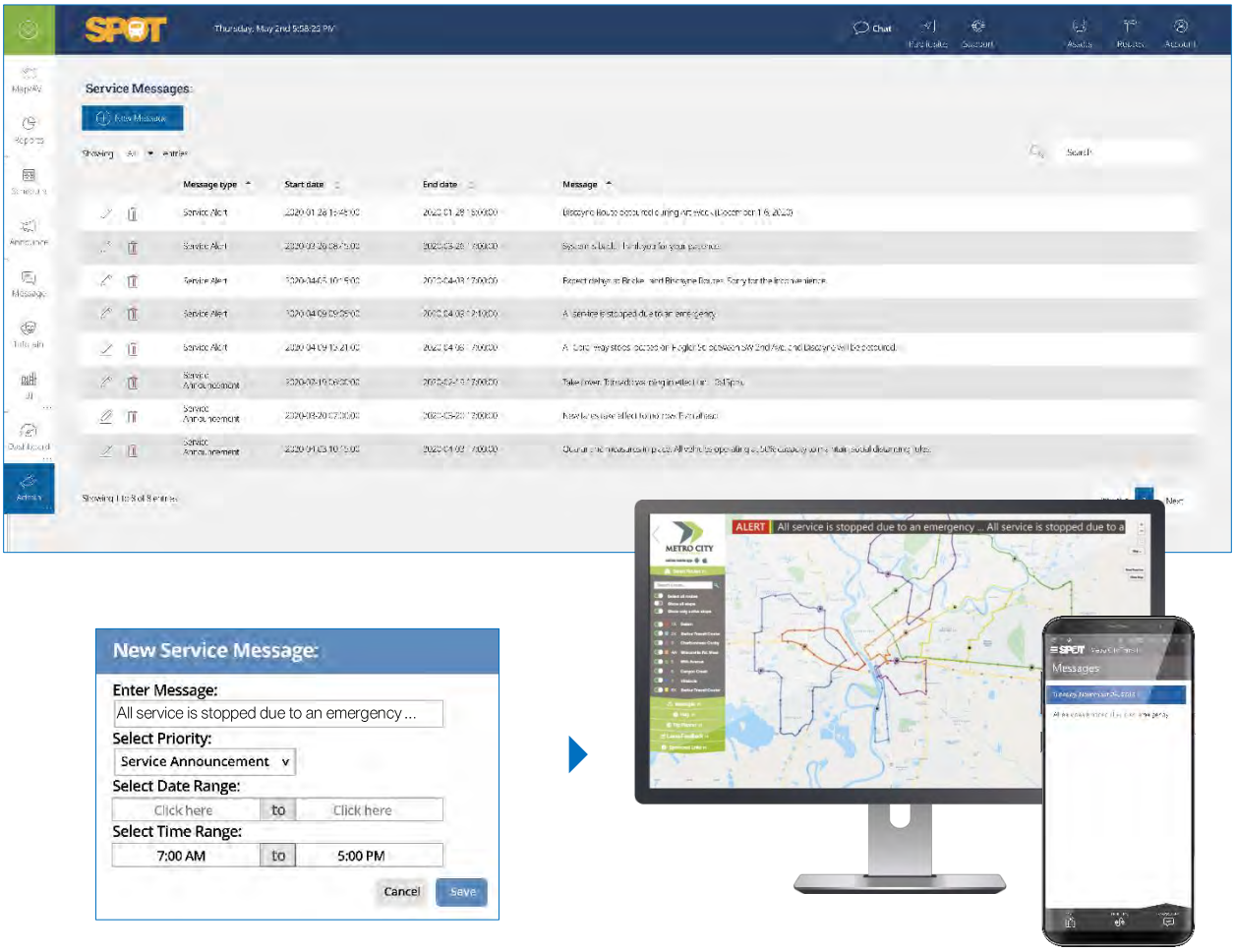


Figure 43: Quickly initiate new messages or manage existing notifications. Notifications deploy automatically to all connected systems such as public-facing websites, mobile apps, and station signage.

Station Manager module
Define stop amenities and information

Stakeholders impacted: *Dispatchers, Operators, Riders*

A feature unique to the SPOT™ intelligent transit system is the inclusion of a Station Manager module. This system provides valuable rider information feature to rider-facing tracking websites and mobile apps that extend beyond merely listing routes and upcoming arrivals.

The SPOT™ Station Manager module ups the ante by serving up additional information and features that your passengers can find useful, including:

- Communicates station amenities such as lighting, shelter type, accessibility options, and more
- Includes photos of the station for visual reference/confirmation
- Provides directions to the station
- Create stop-specific rider alerts
- Display local attractions like banking, restaurants, shopping, entertainment, and more

Providing station details improves rider confidence about their travel itinerary by including helpful information and descriptions about the stop, routes served, and photographic references.

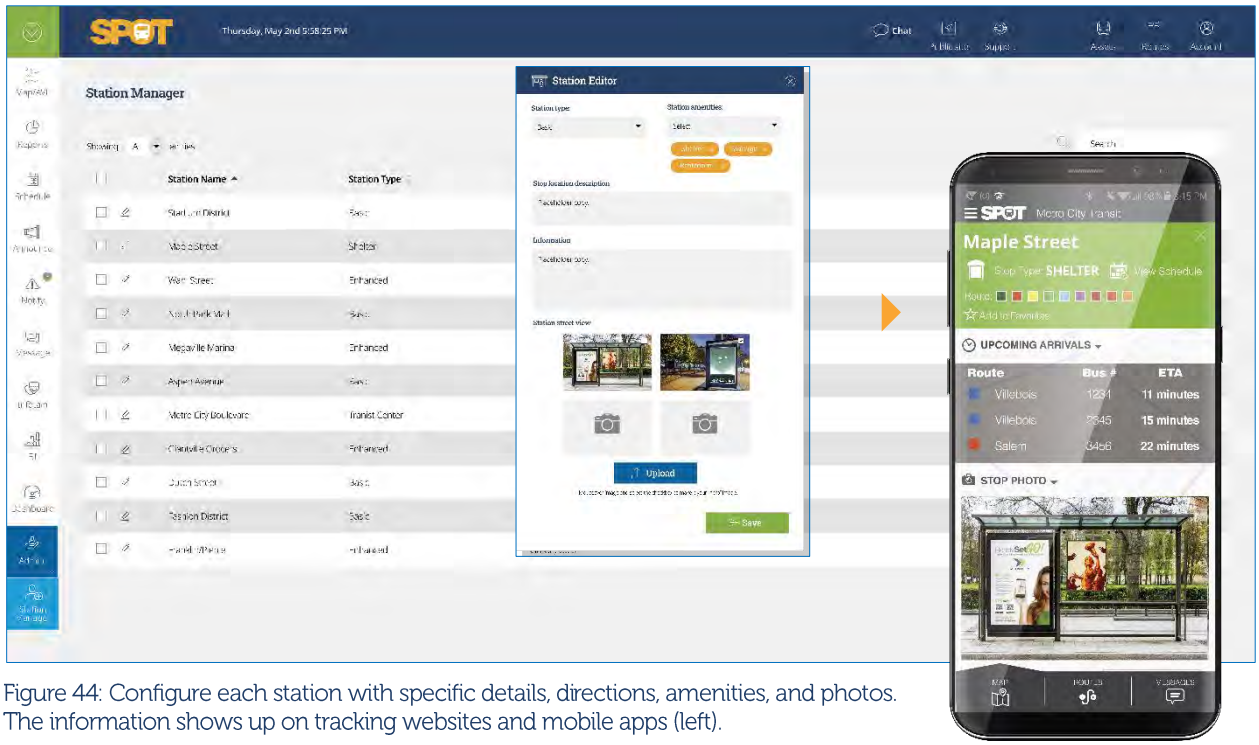


Figure 44: Configure each station with specific details, directions, amenities, and photos. The information shows up on tracking websites and mobile apps (left).

System Alerts module

Stay on top of issues that can impact your operations

Stakeholders impacted: *Administrators, Dispatchers, Drivers*

The system alerts module allows dispatchers to view and filter alerts that have been triggered in the SPOT™ system. These alerts can come from several sources including vehicles, third parties, performance thresholds, exceptions, and other configurable sources. The system alerts module provides an at a glance perspective into incidents requiring attention.

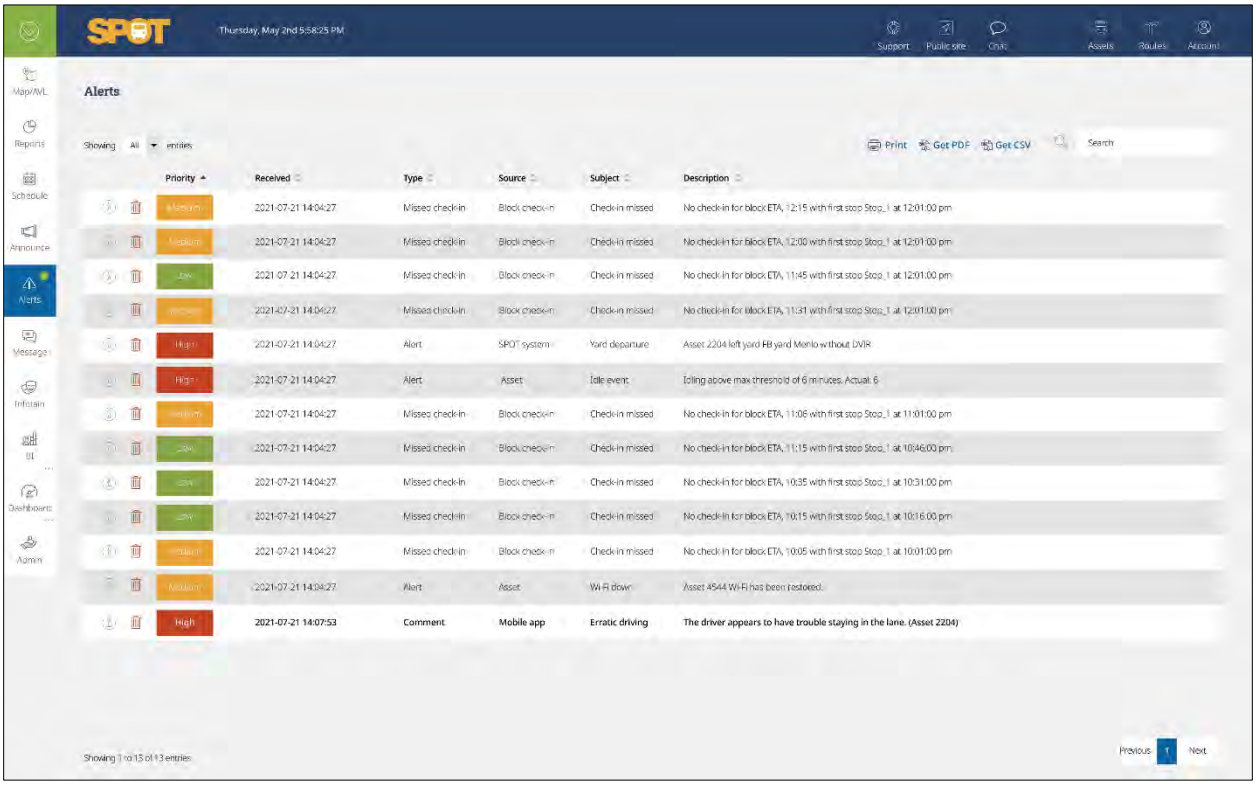


Figure 45: Alerts are color-coded to satisfy pre-defined urgency and severity.
Sort and manage alerts from within this dialog to stay on top of urgent matters.

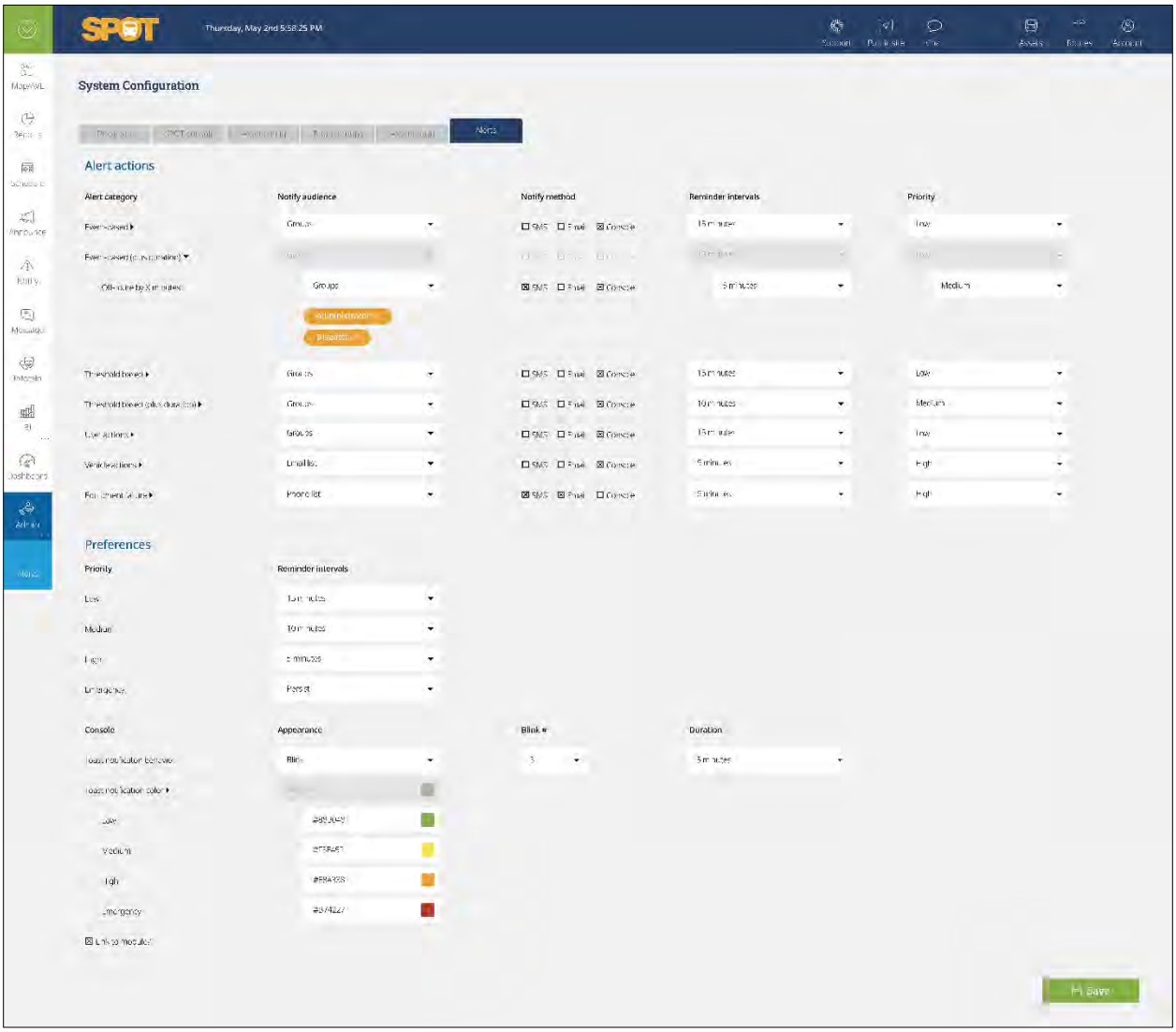


Figure 46: Configure your Alerts to behave according to preferred criterium.

System Configuration module
Fine tune the functionality your SPOT™ system

Stakeholders impacted: *Administrators, Dispatchers, Operators*

The SPOT™ ITS provides GoCOMO with tools to fine-tune the appearance and behavior of both your back-office system and the public-facing bus tracking website. The System Configuration module consists of four separate tabs, each responsible for controlling its own specific set of features:

- Public site
- SPOT™ console
- Asset config
- Route group

Public Site tab:

This set of controls govern the appearance of the vehicle tracking website that riders see when they visit, your agency's site or mobile app. Among the many settings available on this tab include:

- Govern on-screen motion of vehicle assets
- Specify terminology for routes and assets
- Decide whether to include area points-of-interest (attractions) on map
- Choose which menu options appear in the navigation menu
- Opt to show optional features, such as trip planner, mobile app download, rider feedback, etc.
- Upload links to surveys, events, advertising, and more
- Brand the site to your agency's corporate color scheme
- Craft message for vehicle and station LCDs
- Customize scroll speed
- Choose default routes to display

Helpful hint!

For many riders, the Public Site is the primary destination for their travel-related questions and information. Use the opportunity to brand the site with your logo and colors. Leverage optional features such as 'Sponsored Links' to provide additional resources or engaging content.

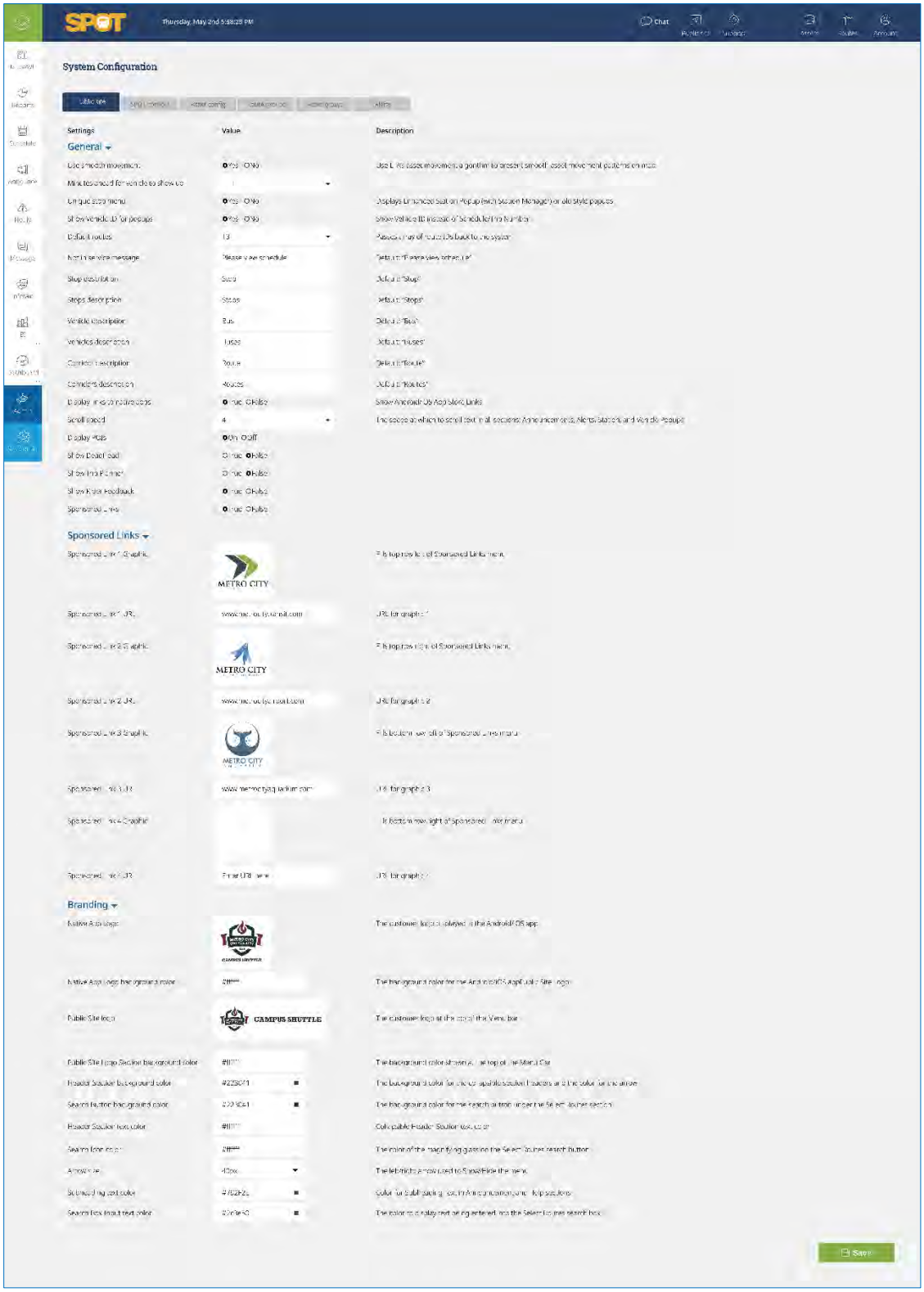


Figure 47: The Public Site tab provides a tremendous amount of customization options to dial in the features and capabilities that best suit passenger engagement goals.

SPOT™ Console tab:

This tab provides the ability to fine-tune the behavior of SPOT™ to satisfy the operating preferences of the City of Columbia's service. Among the settings that can be adjusted are:

- Specify vehicle timing; define early, late, and very late classification in minutes
- Specify colors for vehicle schedule performance, including on-time, early, late, and very late
- Define schedule ranges, including early a.m., peak a.m., midday a.m., peak p.m., and late p.m.

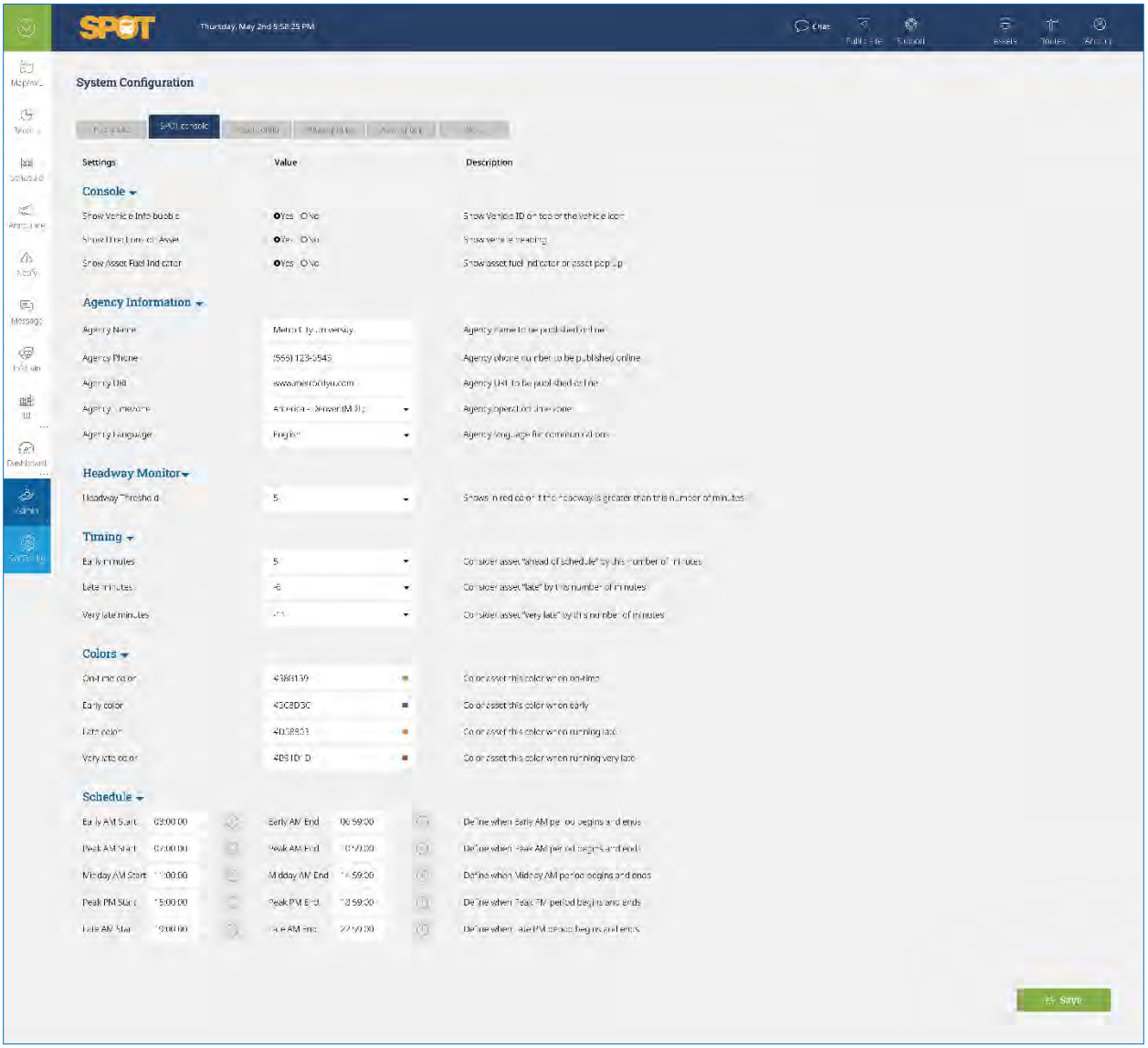


Figure 48: Many settings in the SPOT™ console tab have an impact to both back-office and public-facing systems.

Asset Config tab:

Define the performance of your fleet by configuring the behaviors of onboard hardware and software.

- Define behaviors for a vehicle
- Enable night mode for MDTs
- Define fare categories displayed on the MDT
- Define page duration of onboard Flight Information Display Systems (FIDS) if applicable

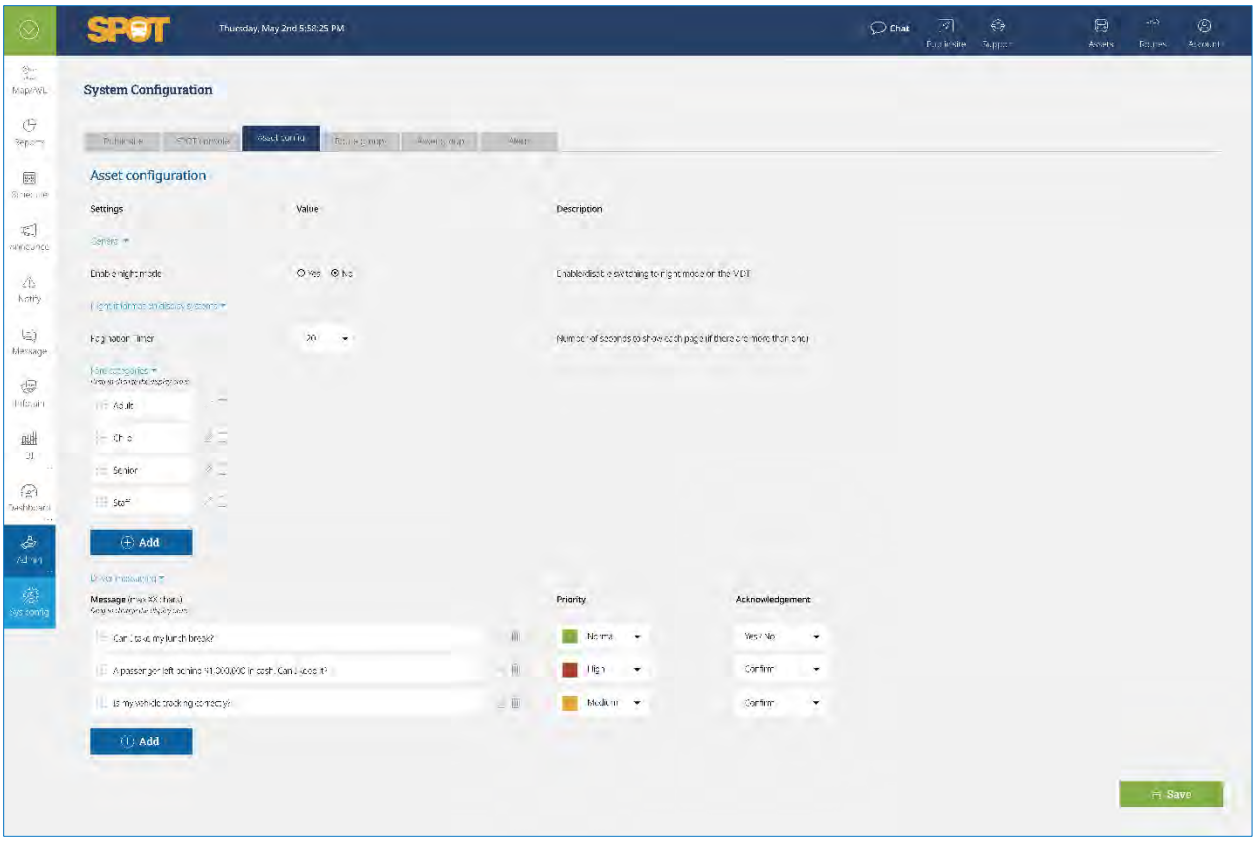


Figure 49: Add, edit, and remove categories for the MDT Fare Collection module. Items added here automatically update on the mobile data terminal to significantly simplify collection of new fare types and special designations.

Route Group tab:

You can define route group by combining multiple routes into a group. This feature displays specific reports and features in a single view rather than per route. For example, should GoCOMO have a morning route and afternoon route and wishes to obtain the performance per stop, the solution would be to create a route group that contains both routes.

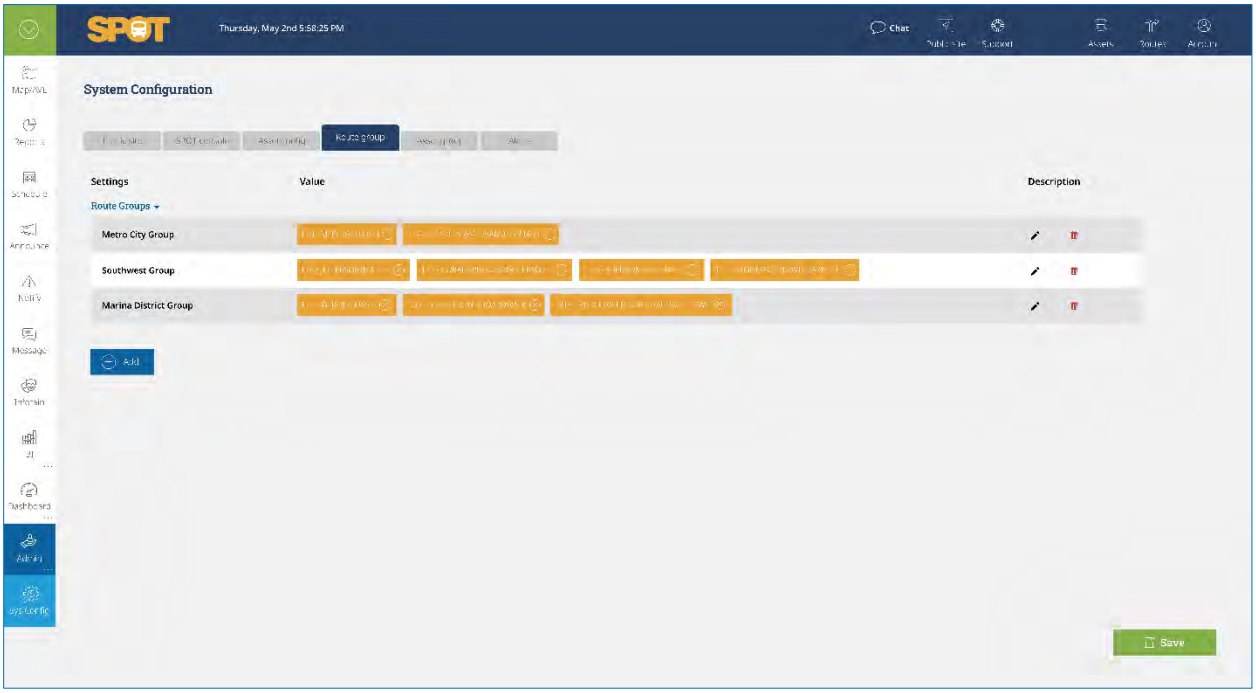


Figure 50: Combine multiple individual routes into new groups to create new views for reporting purposes.

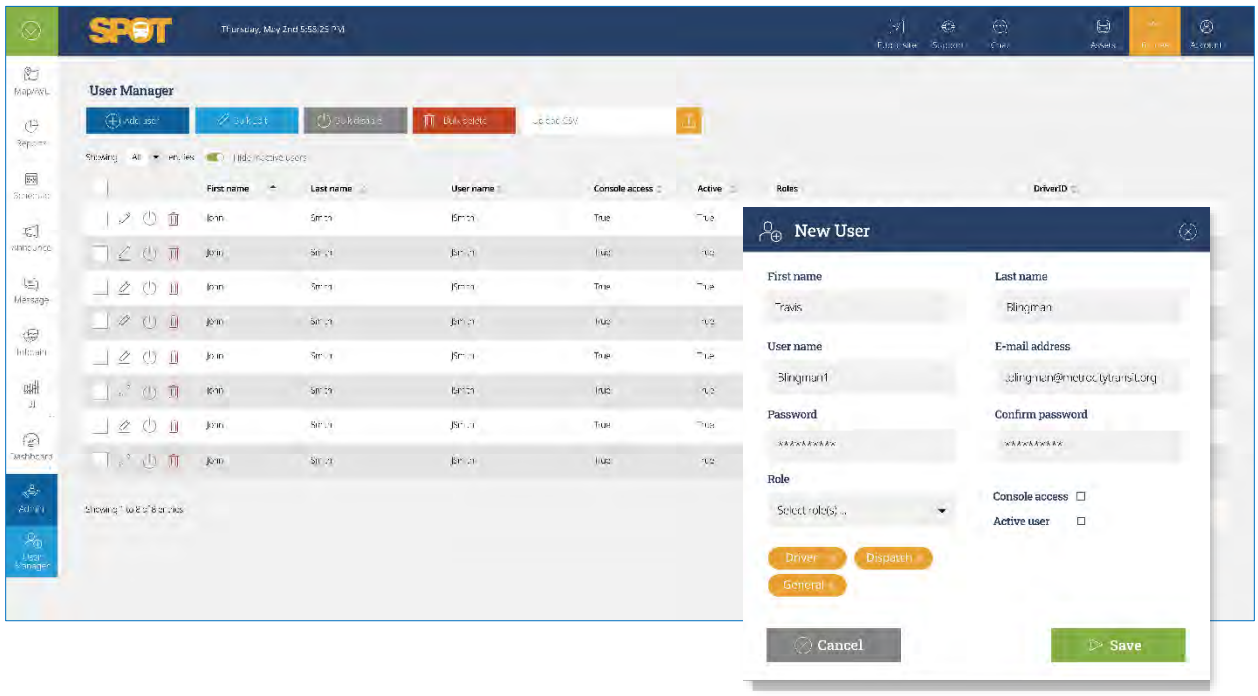
User Manager module

Define who can access and control your SPOT™ system

Stakeholders impacted: *Administrators, Dispatchers, Operators*

SPOT™ provides an unlimited number of user accounts and a straightforward means of managing the access granted to the City of Columbia employees. The User Manager module provides:

- Simplified user management, including adding and disabling of accounts
- Import user from spreadsheet with provided downloadable template
- Assign of usernames
- Determine if a user is active within the system
- Define multiple user roles within the system at one time
- Update/change passwords
- Grant access to the SPOT™ administration console



Helpful hint!

The User Manager supports the import of spreadsheet files in a CSV format.

Required & optional technology packages

[What you will discover]

SPOT™ has a wide range of technology and expansion options that the City of Columbia may choose to implement to meet upcoming needs of its riders and operational mandates.

[Section key points]

- Required: Automatic voice announcements (AVA) package – The City of Columbia will be able to provide clear, automatic, professionally recorded audible messages based on a variety of parameters including geofences, triggers, and pre-defined points. Benefiting the passenger experience with clear messaging while allowing the operator to focus on their core function of driving
- *Optional*: Passenger information display (PIDS) package - With this package, the City of Columbia can deploy displays at key areas utilizing a state of the art content management system (CMS) to communicate with it's ridership including the students, faculty and staff at the various universities in Columbia.
- *Optional*: Solar-powered e-paper digital signage package - Easy to deploy, simple to manage, e-paper signage is an ideal solution to provide real time information at bus stops, transit centers and any location throughout the City of Columbia's service area
- *Optional*: Mobile Video surveillance (REI) – GoCOMO can elevate the safety and security of your passengers and fleet. Improve its day-to-day operations and efficiency with Radio Engineering's MVS system. With advanced hardware, and innovative software easily integrated and customized to meet your fleet's unique needs
- *Optional*: GTFS -RT - The establishment of a standardized approach for information sharing has become indispensable for the success of any agency. GoCOMO will be well-equipped to offer real-time data updates to its partners, utilizing the industry-standard for seamless integration

Automatic vehicle announcements rank as the most desired upgrade to on-vehicle technology.

— 2018 ETA Transit Agency Survey

Required - Automatic voice announcements (AVA) package

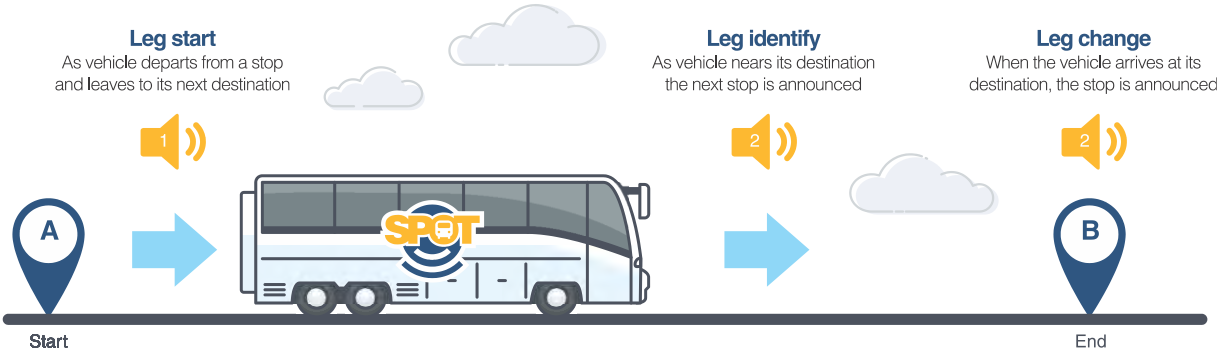
Onboard announcements made easy

Engage riders with SPOT's powerful integrated onboard audio and optional video systems. Featuring an easy-to-use interface, transit dispatchers and managers can quickly generate custom and manage canned announcements that reliably communicate critical stop and service messages to riders.

- Ambient, noise-sensing speakers
- Customized automatic triggers by GPS location or defined events, such as door opens and vehicle stops
- Driver-initiated ad-hoc announcements through mobile data terminals
- Custom geographic dialects and multilingual audio recordings
- Option to integrate with full color, video-capable LCDs

Announcement triggers

Onboard announcements can be configured to play on multiple triggers, including leg start, leg identify, and leg change.



Announcement concatenation

Figure 51: The automatic assembly of various audio files results in a complete announcement of "Welcome to Metro City Transit. You are on the gold route. You have arrived at 34th Street and Elm Avenue. Please don't forget to take your belongings."

Text-to-speech

For customers who prefer to implement a text-to-speech or speech-to-text systems (or augment professional audio recordings), ETA can provide a solution to deliver quality synthesis of written or spoken messages to simulated audio messages.

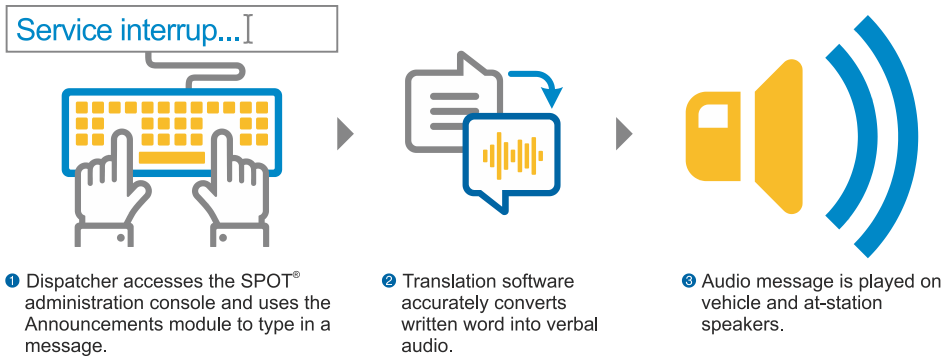


Figure 52: Text-to-speech.

Professionally recorded audio

ETA recommends the use of recorded audio for onboard announcements. The authenticity found in professionally recorded audio provides an improved auditory experience with greater clarity than text-to-speech systems simply cannot match. Factor in multiple languages and dialect support and a national talent pool of voice artists, and recorded audio delivers audio that can capture the authenticity of life in your service area—a simple, and often overlooked way to enhance the value of your agency's brand.

During our initial system setup, we will help GoCOMO define the needs for all system announcements and develop the various pre-announcement, preamble, station, and post-announcement recordings. Our process provides ample time to identify all the components to custom audio recording, including factors such as gender, dialect, language, and refine pronunciations of region-specific names and destinations. The City of Columbia will have enough time to review recordings, identify any potential enunciation issues, and refine the final product before deployment, resulting in a hyper-localized experience from day one.

Common objections to recorded audio:

1. We need to create and deploy audio announcements in real-time.

   This is seldom a case in the day-to-day operations of a transit agency. The odds are that the need for new announcements is known days in advance, and interruptions to service requiring an announcement are often very temporary are better handled through traveler information

websites and display systems. Onboard announcements are built and deployed for automated purposes, not a spur of the moment issue.

2. Recorded audio is more expensive to produce.

   ETA provides recording services at no additional charge for the life of the contract.

3. Recording audio takes too long.

   In most instances, ETA can turn a custom audio recording in one business day.

Learn more about the benefits of pre-recorded audio: etatransit.com/pre-recorded-audio.

Independent display support

Configure messages to automatically play the appropriate message (text, image, or rich media) based on the specific hardware installed at stations or on vehicles. This feature ensures an optimal presentation of information to riders without upgrading all systems to the same equipment.

Figure 53: SPOT's AVA system determines which media to deploy based on the type of announcement systems present at an individual station or vehicle.

Optional - Mobile video surveillance

Strategically placed high-definition camera systems capture every activity on your vehicle and securely download video for review. Both an effective deterrent and capable witness, our rugged security system stands up to the rigors or travel, weather, and overzealous defense attorneys. SPOT™ delivers a premium solution for on-vehicle and at-station video security systems, including:

- Maximum equipment up-time with notifications for system events and failures
- Support for up to 16 cameras and 18 audio inputs
- High definition recording up to 1280x720
- Up to 4TB of removable recording space
- User-friendly search tools and security options to prevent unauthorized viewing
- 3G/4G and GPS-capable with auto-connect Wi-Fi functionality
- Mobile cellular routers with LTE/MIMI/Wi-Fi antenna recorders
- Available automatic uploads whenever the vehicle returns to base
- Optimal network performance with H.264 compression
- SAE-rated steel construction for vandal and impact resistance
- Options for tempered glass and UV coating
- Plug-and-play open architecture system to ensure compatibility with future cellular technology and upgrades
- Available mobile apps

ETA proposes the use of on-vehicle security cameras from REI®. A longtime collaborator with ETA, REI® provides a wide range of on-vehicle video surveillance solutions for public transit, rail, and school transportation. REI® systems deliver tremendous value to transit operations looking to provide additional security, accountability, and peace-of-mind for their riders and employees.

Digital video recorder

REI's DVR records video, audio, and vehicle data via a removable hard drive. Connect to 6 HD surveillance cameras to provide total video coverage in and around your vehicle. Communication module makes upgrading easy for faster communication technology as it becomes available. Customize your recording times or simply start your vehicle to begin recording. The DVR features:

- Durable, compact, and lightweight construction
- Industrial grade hardware
- Quiet, clean fan-less design prevents dirt build-up

- Internal shock and vibration dampening to extend the life of the hard drive
- Easily configured to your requirements
- Endless customization of accessories
- Customizable video quality settings
- Wi-Fi and GPS included (antennas sold separately)
- Environmentally designed: aluminum chassis dissipates heat in extreme conditions; internal heater withstands extreme low temperatures
- High speed USB 3.0 port for a fast transfer of video directly to a computer

Hard drive

REI's removable solid-state hard drives reliably record all recorded video and audio for later playback. Available to configure for wireless access, these durable drives feature:

- Choose capacity from 500GB to 4TB
- Shock resistant construction
- Durable, extruded aluminum chassis
- Vibration dampening integrated into housing
- Integrated heater for operation to -40°F
- No docking station required – USB 3.0 port on SSD housing for direct connection to a host PC
- Activity and communication lights for visual verification of operation and PC connectivity
- Key switch locks USB port preventing unauthorized access to SSD contents

Cameras

All REI cameras are designed to operation at extreme temperatures, withstand power fluctuations, and handle the vibrations found in the toughest mobile environment. Your on-board security system may feature the following high-definition cameras: *

Figure 54: From L to R, Eyeball AHD, Dome AHD, and Minibox AHD, cameras.

** depending upon final vehicle assessment/review*

Table 2: REI MVS camera feature and specifications.

Feature	Eyeball AHD	Dome AHD	Minibox AHD
True wide dynamic range	3	3	3
1080p/720p HD resolution	3	3	3
Day/night viewing	3	3	3
Interior use	3	3	3
Exterior use waterproof connection	3		
Proprietary optimized audio	3	3	3
Optimized IR for eliminating hot spots	3	3	3
Adjustable camera angle	3	3	3
Tamper resistance	3	3	3
Water resistance	IP69K	IP67	IP65
Gorilla glass	3		
Wide FOV option	3	3	
Ultra-wide FOV option			3
Adjustable audio	3	3	3

Software

REI's user-friendly A.R.M.O.R.™ software enables you to view and search your video and provides access to a variety of vehicle data. This video suite, provides:

- View and search video from hard drives, SD cards, USB thumb drives, archived video
- Remote connection to DVR to wirelessly view recorded or live video (optional hardware required
- Search by alarms, speed, accelerometer, GPS geofence, G-force threshold, and user-selectable inputs
- View video recorded in high definition from all installed HD cameras
- Graph speed, acceleration, hard braking, and other vehicle data to evaluate driver behavior and vehicle performance
- Pinpoint vehicles on routes to view video at specific time and location.

Optional - Passenger information display package

LED, LCD, and kiosks deliver larger-than-life engagement

ETA's passenger information display systems (PIDS) provide incredible value and versatility to your rider communication efforts. These systems help to remove the uncertainty inherent to transit operations by providing riders with real-time updates, interactive maps, accurate arrival predictions, public service information, as well as the opportunity for revenue-generating advertising.

When integrated with the SPOT™ platform, PIDS are updated automatically whenever a change is executed. This automation provides a single point of control to roll out critical updates to your passengers, a key benefit to transit agencies looking to streamline operations and realize improved efficiency and customer satisfaction.

Options abound with ETA Transit's PIDS package, allowing GoCOMO to pick and choose the right display options for its budget and passenger information needs, including:

- Variable message interior and exterior LED signage
- High-definition LCDs
- Custom kiosks with an optional interactive, touch screen interface
- Solar-powered e-paper displays

Variable message interior and exterior LED signs

Another component to ADA compliance, interior-mounted variable message signs seamlessly integrate with single sign-on capabilities and automatic "next stop" announcements.

Figure 55: Add LED signage to vehicles and stations for improved communication and ADA compliance.

High-definition LCDs

Make an impact with onboard and station rich-media LCDs. The epitome of versatile, our high-definition, transit-tested monitors deliver public service announcements, play advertisements, and display real-time schedule and arrival predictions.

ETA will work with GoCOMO to customize the design of its desired information. This process significantly improves communications, increases rider satisfaction, and serves as a reliable platform for the creation of advertising and promotion revenue opportunities.

Figure 56: Provide riders with important system updates, rich content, and targeted advertising.

Exterior signs and kiosks

These rich-content capable, Internet-connected displays are managed through your SPOT™ administration console via the announcements module and provide numerous display options. The same messaging and information displayed on your vehicles automatically presents on displays—*without the need for a separate interface or additional production*.

Figure 57: Deliver personalized information and rich media content via vibrant, customizable displays, and kiosks.

Optional - Solar-powered e-paper digital signage package

Much more than a sign of the times

Papercast® e-paper signs provide a highly flexible, powerful communication platform for transit operators seeking a reliable communication platform that mixes next-gen screen display technology, modern design aesthetic, and versatile real-time information capabilities.

ETA Transit's SPOT™ software suite enables all the displays in the system to be monitored and managed from a central location. Solar-powered e-paper displays provide travelers with reliable real-time information in the most cost-effective way—no matter a bus stop location.

Unleash the potential of digital e-paper displays:

- High resolution display (1200 px X 1600 px) supports real-time arrivals, maps, QR codes, and more
- Maintenance-free and no battery replacement necessary
- Installs on existing structure/pole; no power or data cabling required
- Supports multiple sign configurations, pages, and layouts
- Ultra-low-power LEDs controlled by motion and light sensors
- Supports text-to-speech for visually impaired riders
- Online update and monitoring
- Custom branding with agency logo and colors
- Cellular, Wi-Fi, or Ethernet connectivity

Figure 58: Papercast® single sign e-paper display.

Simplified installation

Free from costly infrastructure demands, Papercast® bypasses expensive network and power wiring requirements in favor of solar panels and wireless connectivity.

ADA-compliant

High contrast displays and text-to-speech capabilities improve the travel experience for visually impaired travelers, helping to satisfy ADA regulations.

Amber alerts

Papercast® displays can provide an interface through the available API to broadcast Amber Alerts to all connected signs.

Fonts

E-paper displays are not limited to any kind of different font types or sizes. Users can change the fonts via the Papercast® CMS. Due to modularity of the font sizes displays, customer can choose different font types and sizes therefore the legibility of the screen is line with the guidance of minimum character sizes in the Americans with Disabilities Act (ADA) compliance requirements.

Text-to-speech (TTS) functionality

The Papercast controller board supports TTS using the Nuance software solution (other providers with a software development kit (SDK) can also be integrated (i.e., Acapela)). The TTS engine leverages neural network techniques to deliver a human like, engaging, and personalized user experience. It enhances any customer self-service application with high quality audio.

The TTS application is controlled by display application (written in NODE.JS) and can be tailored to provide information such as:

- Name of stop
- Current time
- List of arrivals (either first arrival, multiple arrivals etc)
- Stop/route status
- Incidents and other notifications
- Any other information available at the stop

Triggering of the TTS can be through press of a button on the display, via remote switch (such as pushbutton connected to the display) and wirelessly.

The Papercast displays have an option for embedded loudspeakers (2x 3W – compliant with US transport standards) with an integrated amplifier or through an external speaker such as an ADA compliant pushbutton loudspeaker. In the latter case sound is amplified through a pushbutton device to the required level.

The TTS engine supports multiple languages. English is the default language, however there is optional support for Spanish, Chinese, French, Italian and other major languages.

Figure 59: Weather-resistant Papercast® displays reliably perform in a variety of weather conditions, from cold and wet to hot and dry.

All-weather capable

The elements are the most significant variable in any transit environment. The Papercast® display is what we like to say, “postal ready.” Through rain, sleet, snow, and hail, nothing will keep your riders from delivering all the real-time arrival predictions, relevant system alerts, and information they need to arrive from points A to B.

These signs are well-suited for extreme weather climes. The units operate in minus temperatures fond in Scandinavia and Japan, as well as high-temp environments such as Abu Dhabi, Kuwait, and Dubai, where heat and sand is very much a factor.

This durability includes solar panels. The construction of these sturdy boasts the latest materials and state-of-the-art technology and are capable of charging on days with overcast skies on cold and hot days alike.

- Operating temperature (BW display): -5˚F–158˚F
- Operating temperature (grayscale display): 32˚F–122˚F

- Operating temperature (solar panel): -45˚F–176˚F
- Protection: IP65

Energy efficient

Exceptionally energy efficient, a single charge can power the signs for weeks—a perfect solution for areas prone to sustained cloud cover. Further enhancing power conservation, the Papercast® employs intelligent motion-sensing technology only turns on the display when it senses a nearby rider.

- Power: 12V DC
- Power consumption: 50 mA–80mA
- Charge cycles: 2,000
- Utilizes 36 times less power than LCD equivalent signs

Powerful content management

Papercast's powerful cloud-based content management system allows you to manage your e-paper displays in real-time remotely. The intuitive user interface makes the system easy to master, so you can effortlessly control every aspect of every Papercast® display across your network—individually, selectively, or collectively.

- Easy onboarding
- Create and customize content
- Publish content instantly or on a schedule
- Receive notifications of attempted vandalism

It offers straightforward and instant integration with open standards such as GTFS, GTFS RT, and SIRI for real-time passenger information, with custom API integration available for other data formats. The platform hosts a broad range of predefined content apps for additional travel information such as service schedules, maps, timetable alterations, and emergency notices. Users can add custom content apps and widgets, as well as develop their own using javascript Node.JS.

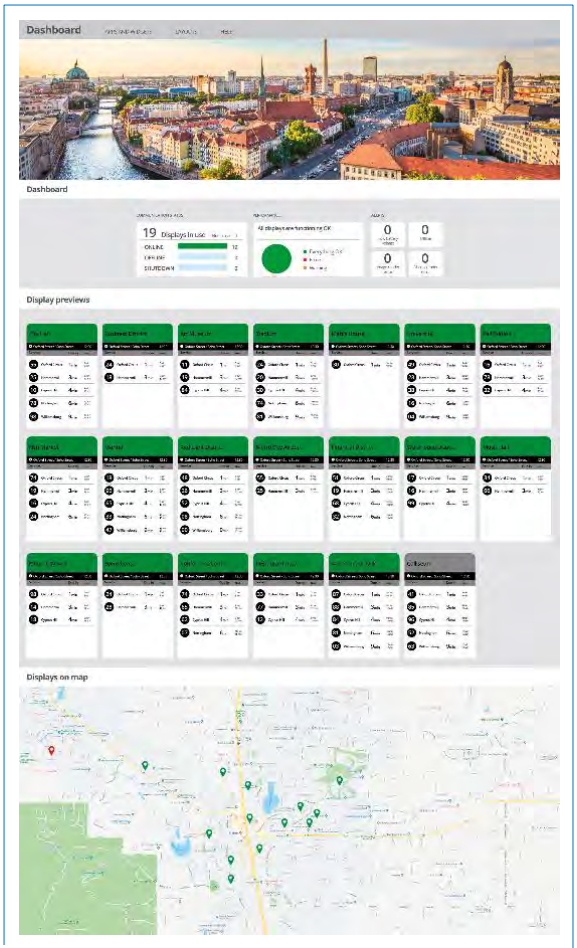


Figure 60: View the status and current display of all your Papercast® displays via the CMS dashboard.

The management system supports day-to-day and routine operation of the Papercast® displays. You can control, monitor, report, and receive notifications on all aspects of display performance, including status, content, connectivity, power management, auto-diagnostics, movement detection, solar charging, and external sensors.

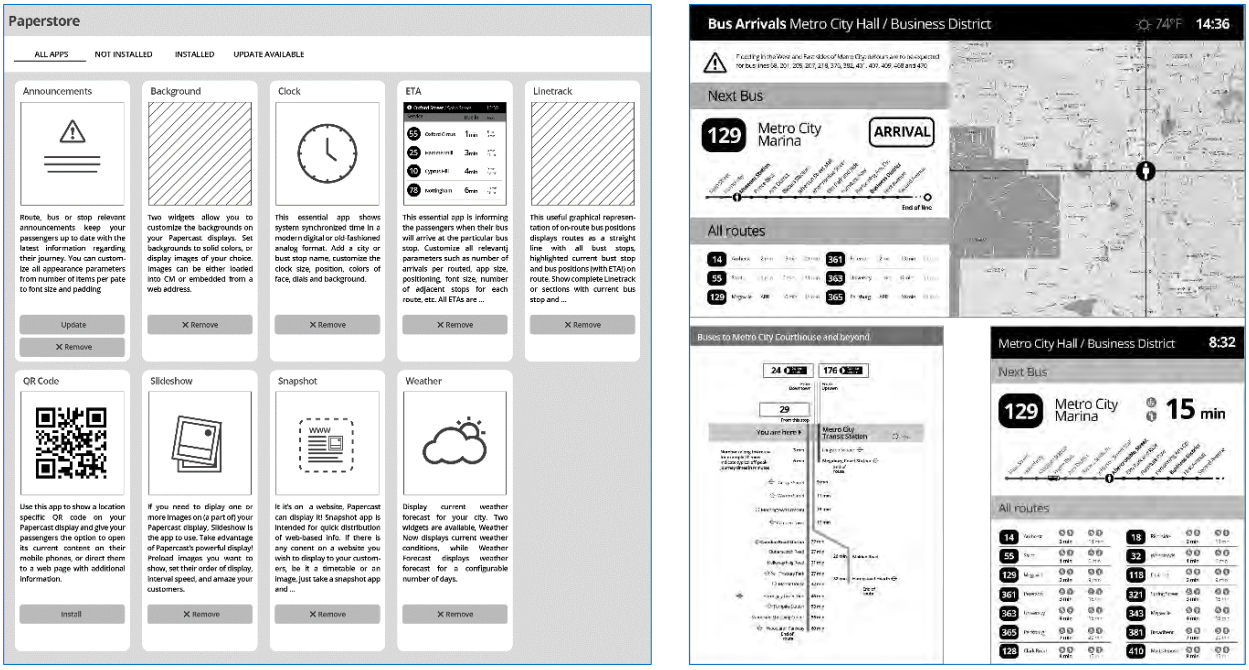


Figure 61: Add apps, widgets, and personalize the display with multiple layout options.

Wide utilization

Papercast® sign technology is in place in major metropolitan, high traffic locales such as:

- San Antonio
- London
- Kuwait
- Berlin
- Jerusalem
- New York
- Miami
- Cambridge
- Paris
- Japan
- Pittsburgh
- and more!

Theft-deterrent

Papercast® can be securely displayed to almost any surface and discourages theft using sturdy, steel mounts, and tamper-resistant screws/bolts. Additionally, the technology itself has little repurposed value outside of a duly authorized data feed, making theft of the sign undesirable outside of the transit market. In all Papercast's history, there are only two recorded instances of theft among thousands of installed signs across the globe.

Figure 62: Detail view of the anti-theft assembly and unit construction.

Long-term value

An investment in ETA Transit's Papercast® solar-powered e-paper displays is a forward-thinking decision that carries environmental and economic impacts that extend far beyond the initial investment price.

The solar-powered batteries can operate the display for weeks without the need to recharge, are transit tested, and sturdy enough to handle the demands of riders—making them nearly maintenance-free. The inclusion of motion-sensitive capabilities ensures that the display shuts off when no one is around. In short, your agency does not have to pay for an electric bill each month for these signs, which saves money.

Papercast® e-paper signs represent an investment in the future and a sound approach to both fiscal and environmental responsibility. These displays are more than just a sign of the times; *they signal a modern*

approach to a changing world, one which demands foresight, wisdom, and a desire to serve the customer at every turn.

Display solutions for any situation

Should the City of Columbia wish to extend its information display capabilities and "wow" their riders, it has more options to choose from, including:

Figure 63: Multiple Papercast® display options. From L to R: 13" double, 13" triple, 23", 32",42"(top right) and 57" (bottom).

The advantages of Papercast® e-paper signs over traditional LED displays

Low maintenance

Papercast® displays require little investment in installation expenses, support high-resolution graphics, provide real-time updates, and deliver exceptional readability in all lighting conditions. These durable signs do not require new wiring or infrastructure, making them easy to install, upgrade, or replace.

Brand enhancement

The e-paper display provides a tremendous amount of customization in the form of graphics, font selection, and information configuration. The sign casing itself can be colored to match your agency's colors; logos are to the display area and shell. Custom branding has the effect of making the sign feel

connected to the whole transit system and mitigating any concerns or competition from other transit providers.

Improved legibility

In our view, a wide, narrow sign presents legibility challenges. When positioned high up on a post, there is immediate visual competition from the sun, clouds, and overhead objects can affect the clarity of the display; riders must crane their necks toward the sky to view updates, which can cause discomfort.

ETA's solar-powered e-paper solution is uniformly visible day or night, and strategically positioned at eye level for ease of viewing. Type and graphics can be customized to meet preferences (where LED signage is the fixed height).

Figure 64: Papercast® e-paper screen technology delivers large, high-contrast displays in any lighting condition.

Flexibility

The e-paper solution provides a customizable interface and content management features that help transit agencies fine-tune the presentation to provide the right amount of information to riders. It supports the use

of multiple screens, graphics, maps, and of course, a real-time feed of data from your transit operations—everything seamlessly managed and automatically updated from the SPOT™ administration dashboard, with little to no manual intervention.

Optional - GTFS real-time (GTFS-RT) package

Clarify the passenger journey

You've made the investment in an intelligent transit system, now share your system data and arrival predictions with the world by converting your data into the GTFS-RT (real-time) format. A universal standard, the format allows you to share data with a wide range of providers, deliver more accurate arrival predictions, improve communications with riders, and easily integrate with numerous hardware and software platforms.

Why adopt the GTFS-RT standard?

- Tips the balance of power to transit operators (more choices)
- Universal data format
- Simplifies data sharing with connected systems like stop signage, onboard infotainment displays, apps, and more
- Removes the need to write custom translators for proprietary APIs
- Provides up-to-date information with Google® trip planning and map services
- Streamlines integration with 3rd party systems

Installation & training

[What you will discover]

ETA has a lengthy track record for delivering on-time and on-budget deployments of its SPOT™ solutions. Our proven approach to deployment will help the City of Columbia to significantly mitigate surprises for a smooth transition that accounts for pre-launch, system construction, and training.

[Section key points]

- Experience: ETA Transit's experience in deploying 100's of projects will benefit the City of Columbia by providing a stream-lined, thorough approach to project installations. Leveraging our extensive project deployment experience, the GoCOMO system will be deployed and ready for revenue service within 8 weeks from notice to proceed.
- Quality: With an emphasis on testing and verification, the City of Columbia will be confident in the reliability of the system and the data it produces. ETA places high priority on testing and verification to achieve optimal functionality of the SPOT™ ITS system. We believe that transparency is critical in any project deployment, and we welcome the opportunity for GoCOMO to witness our testing procedures
- Structured Training: GoCOMO's training program will be divided into two components: classroom-based instruction and real-world training, using customer experience advocates to work alongside staff to reinforce the concepts learned

Let's look at the gameplan!

Improving the rider experience (46%) rates as the primary motivation for system upgrades and improvements.

— 2018 ETA Transit Agency Survey

An iterative process

A rigorous methodology for consistent results

Since its founding in 2003, ETA has never failed to deliver on a deployment timeline. With over 100 implementations on our resume, that is an exemplary track record of performance. Besides having a group of dedicated employees, and strategic partnerships with installation vendors, the key to our success is our rigorous, seven-part approach to project management.

To ensure the timely completion of your SPOT™ ITS system, ETA will provide a detailed project management plan that will document the responsibilities and schedule for each stage of the project.

A seven-part project deployment strategy:

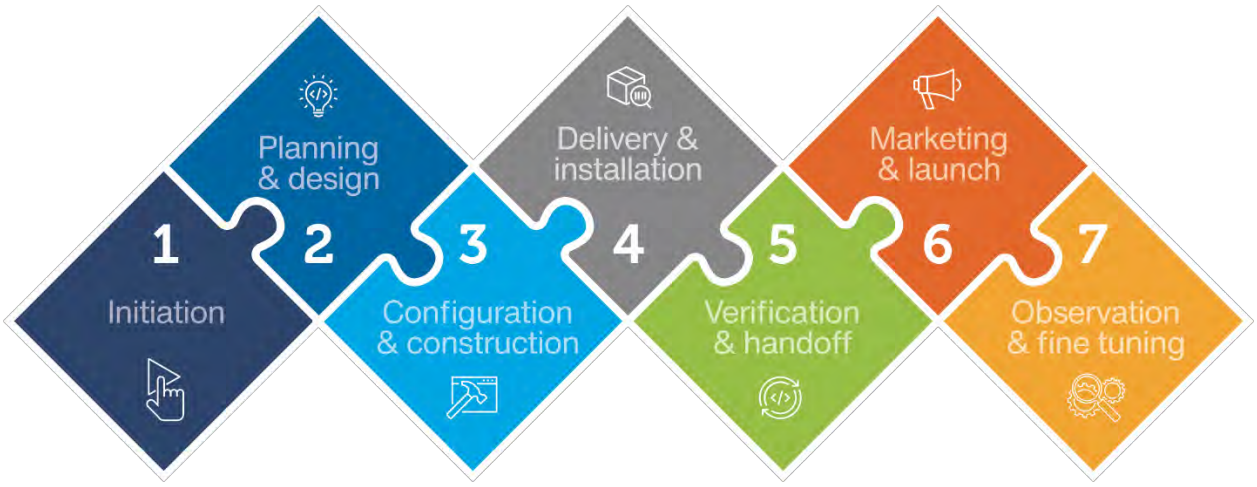


Figure 65: The benefit of our approach is twofold: Clearly defined steps to thoughtfully introduce the SPOT™ technology to your operations. The iterative process helps reveal more truths about your environment to make continuous improvements along the way.

Preliminary work plan and schedule

As a preliminary step in the deployment of the SPOT™ system, ETA has developed a high-level project plan based on an anticipated notice to proceed of September 01, 2023 and deliver a core system (excluding options) inside of 8 weeks. Within five days of NTP, ETA will spin up GoCOMO's administration portal. This early access to a critical SPOT™ system allows our team to work with your transit planners to dial in GTFS data and build familiarity with the system.

	Weeks											
Phase	1	2	3	4	5	6	7	8	9	10	11	12
Initiation	✔											
Planning		✔	✔	✔	✔							
Construction			✔	✔	✔							
Delivery						✔	✔	✔				
Verification							✔	✔	✔			
Marketing									✔	✔		
Observation									✔	✔	✔	✔

Table 3: In most cases, a complete SPOT™ system can be deployed in as little as 12 weeks.

Witness testing

Testing is the name of the game, at ETA with numerous testing and acceptance procedures baked-in to our project management plans. We perform exhaustive type testing on candidate components before they ever enter our materials list, and we systematically evaluate these systems into each specific hardware configuration throughout the process. You can be assured that ETA will test the City of Columbia's solution multiple times before deployment.

We encourage the City of Columbia to witness our testing of its system components either on-site during deployment, or pre-deployment at our Boca Raton, FL factory. Transparency is critical, and you will have every opportunity to ensure that its new SPOT™ system performs to its stated specifications.

We will provide GoCOMO with access to ETA's customer support portal so that it may create and track issues every step of the way.

Documentation

All aspects related to your SPOT™ ITS will be thoroughly documented, including core components and system software, as well as additional features and components. The documentation will be developed for users of a wide range of technical competencies, and include considerations for vehicle operators, dispatchers, network support staff, area managers, administrators, and maintenance technicians. The information provided will range from technical schematics, and part lists to step-by-step instructions on the use and maintenance of systems and equipment.

Unless specifically requested, ETA will provide all system documentation in a digital PDF format via online download or USB flash drive.

Key concept!

Communication is an essential component of any successful project deployment, and ETA's project management team has built-in the necessary checkpoints and feedback processes to ensure that the City of Columbia has every opportunity to voice concerns or provide input.

Project timeline

Upon notice to proceed (NTP), ETA will generate a comprehensive Gantt chart that details each stage of the City of Columbia's project. This timeline will follow the framework of our six-step project management process.

Phase #1: Initiation

Entrance criteria: Signed contract with notice to proceed

ETA roles: Administrator, customer experience advocate, project manager, sales representative

GoCOMO roles: Administrator, dispatcher, maintenance, marketing, operator, planner

Among the important items to be completed before proceeding to the next phase include:

- Welcome kit
- Customer data register
- Bill of materials (BOM)
- Order parts
- Schedule site visit
- Wireless study (as needed)
- Pre-installation vehicle survey
- Operations analysis meeting
- **Milestone: Project kick-off meeting with the customer**

Phase #2: Planning & design

Entrance criteria: Project kick-off meeting

ETA roles: Project manager, Design engineer, sales representative

GoCOMO roles: Administrator, Maintenance manager, Planner

Among the important items to be completed before proceeding to the next phase include:

- Create SPOT™ portals
- Conduct initial SPOT™ console training
- Verify route/GTFS data with customer (first pass)
- Update BOM
- Develop block diagram
- Develop Installation guide (pre-installation section)
- Update BOM and purchase orders (as needed)
- Update official project schedule
- **Milestone: Design review meeting with the customer**

Phase #3: Configuration and construction

Entrance criteria: Design review meeting

ETA roles: Project manager, customer experience advocate

GoCOMO roles: Administrator, planner

Among the important items to be completed before proceeding to the next phase include:

- Configure SPOT™ console settings
- Configure SPOT™ public tracking website app
- Configure optional system components (e.g., APC, AVA, AVM, etc.)
- **Milestone: Configured SPOT™ System**

Phase #4: Delivery & installation

Entrance criteria: Gap analysis and inspection test reports completed

ETA roles: Project manager, customer experience advocate

GoCOMO roles: Administrator, maintenance, dispatcher, operator, planner

Among the important items to be completed before proceeding to the next phase include:

- Customer witnessed static test
- Customer witnessed dynamic test
- Deliver maintenance manual

- Deliver SPOT™ console user manual
- Deliver operator (driver) user manual
- **Milestone: Customer review of documentation**
- SPOT™ console user training
- SPOT™ operation (driver) training
- SPOT™ maintenance training
- **Milestone: Testing and training complete**

Phase #5: Verification and hand-off

Entrance criteria: Documentation, installation, testing, and training completed

ETA roles: Project manager, customer experience advocate, sales representative

GoCOMO roles: Administrator, operator, planner

Among the important items to be completed before proceeding to the next phase include:

- Customer First Usage – Discover what you know

Phase #6: Marketing and launch

Entrance criteria: Burn-in period complete and system hand-off to GoCOMO

ETA roles: Project manager, marketing

GoCOMO roles: Administrator, marketing

Among the important items to be completed before proceeding to the next phase include:

- A teleconference between the City of Columbia and ETA marketing teams
- Develop a launch plan and schedule
- Create and deliver marketing materials to GoCOMO
- **Milestone: Launch to public**
- **Milestone: Final hand-off to GoCOMO**

Phase #7: Observation and fine tuning

Entrance criteria: Review system performance from launch and provide necessary guidance and support to ensure proper use of systems, accuracy of data, training, and other performance concerns.

ETA roles: Project manager, support

GoCOMO roles: Administrator, dispatch, planner

Project role definitions

The key to any deployment's success is to understand the nature of the project and assign the appropriate staff members necessary to achieve a timely and successful launch. These individuals should possess the requisite understanding of key concepts and priorities and actively contribute time, insight, and wisdom to the specific operational goals. The definitions of the essential roles in this project are listed in the table below.

ETA Transit

Role	Description
Administrator	A C-level position capable of making contractual agreements for the company.
Customer experience advocate	Works hand-in-hand with the GoCOMO to enhance the ownership experience.
Customer service representative	Makes the necessary connection between customer and support
Design engineer	Develops system design and related documentation
Installation manager	Supervises installation crews and coordinates resources with customer
Installer	Installs and configures vehicle and station hardware
Marketing	Assists in the promotion and communication effort for new system launches
Project manager	Guides the overall project, allocates resources, and coordinates with customer
Sales representative	Point of contact for sales, upgrades, and project-related concerns
Technical support	Works to address customer concerns and resolve performance issues

[GoCOMO]

Role	Description
Administrator	Primary point of contact; power to make contractual and financial decisions
Dispatcher	Communicates with the driver; facilitates day-to-day operational tasks
Maintenance	Ensures that vehicles and connected systems are in proper working order
Marketing	Promotes transit agency to the service area
Operator	Drives vehicles
Planner	Creates and manages routes and service for the transit agency

Project status meetings

ETA delivers written status reports upon the completion of key milestones or at agreed-upon intervals. These communications are detailed explanations in a change of scope, challenges encountered in post-

implementation, timeline updates, budgetary concerns, and related information, which may impact the delivery of the system.

Project team

We have assembled our best and brightest personnel to shepherd the City of Columbia's SPOT™ deployment.

Contracts, negotiation, and billing

Nicole Castonguay

- Over 15 years of experience in customer service, management, and accounting
- Serves as the company's CEO and is the majority shareholder
- Advocates for customers. Ensures customer satisfaction

Project management

Josh Adler

- Studied Project Management at Florida Atlantic University
- Experienced business analyst
- Prior work with Motorola®, The Answer Group®, and Duty-Free America

---

Lead systems architect

Stephen Gunning

- Over 15 years of experience providing transit technology
- Serves as the company's vice president of systems and support; giving leadership to the QA and customer support groups
- Has successfully deployed over 50 transit technology projects
- Expert in software development, automation, and quality assurance
- Ensures that the company meets the stated SLA for response times and system availability

---

Lead project engineer

James Warren

- Over 20 years of experience delivering complex transit technology solutions
- Provides project engineering leadership and technical support to the project
- Analyzes system requirements and ensures that project design meets specifications

---

Customer experience advocate

Graham Saunders

- Over 25 years of experience in software engineering, system testing, and quality assurance
- Dedicated to the GoCOMO project and is responsible for the prompt acknowledgment of customer support requests
- Interfaces directly with customer staff to provide seamless customer support
- Provides fanatical customer service

System administration

John Rodriguez

- Over 15 years of systems administration experience
- Expert in Windows, Unix, and Linux operating systems. Expert in database administration
- Ensures that production systems are in good working order, plans configuration management, and executes system updates

---

Hardware engineering

Alshine Mondesir

- Electrical engineer, embedded software engineer with over 15 years of experience delivering transit technology solutions
- Analyzes system requirements and ensures that project design meets specifications
- Performs installation training and field support

Leon Liberty

- Acts as the company's manufacturing and production coordinator
- Develops bills of material and technical drawings
- Ensures that the system design meets GoCOMO's stated specifications
- Supports the quality assurance and technical support groups

---

Manufacturing, shipping, and receiving

James Bevel

- Serves as the company's manager of production and inventory control
- Assists in customer support (ServiceCloud chat)
- Develops knowledge base articles and videos
- Ensures that GoCOMO parts are correctly tested, kitted, and shipped

---

Customer experience advocate

Taylor Tanksey

- Serves as primary contact for technical issues
- Proactively monitors system to identify potential problems
- Advocates for GoCOMO on support-related concerns

Sales contact

Jose Mostajo

Business Development Representative

Phone: (561) 288-1930

Email: jmostajo@etatransit.com

- Your point of contact for sales-related matters
- Works with GoCOMO to define a technical road map including future expansion technology

---

Training

Focused, role-based instruction

ETA Transit defines a successful training experience as one where the participants receive enough instruction to perform their duties within the SPOT™ ITS system effectively. It ought to be a polished, repeatable approach that provides a blueprint for any trainer—either those experienced with SPOT™ or those new to the role—to effectively conduct a session and achieve the intended result.

The timing and location of the training will be negotiated as part of the contracting phase and may involve either on-site or online instruction.

Bus in a Box

As an option, ETA supplies a "bus-in-a-box" (BiB) to be used for testing and training purposes. The rugged case can include all of the onboard equipment supplied in the project (sometime miniturized for space considerations). Very few customers elect to include the APC as it requires a more permenant/stationary structure to house. Typical components in the BiB include: the VLU, MDT, infotainment screen, pre/post trip mobile device, microphone (used for radio integration) speakers, covert alarm, and interior LED.

Figure 66 Bus in box - Portable training aid for on-board bus technologies

Role-based curriculum

ETA has modeled the education in the SPOT™ system like that of a school curriculum and segmented by job role or title. This targeted approach is designed to keep your staff attentive and focused on learning the skills and functions critical to the daily execution of their responsibilities. The training is broken out into the following sessions:

- Planner
- Operator (driver)
- Dispatcher
- Administrator
- Maintenance

▸ Reference Project role definitions for more information.

Administrator training overview

The administrator training session provides in-depth instruction on the use of the Reports module, so that leadership can accurately manage and obtain the information needed to make informed operational decisions.

- On-time Performance module training
- The daily schedule performance
- Understanding How to Validate Data
- Working equipment
- Valid schedules
- Proper sign-in (system activity)
- Proper route execution
- Breadcrumbs
- Serviced stops and stop times
- Post-processing requests
- Schedule adherence reports
- Headway reports
- Driver performance
- Automatic passenger counter reports
- APC ridership
- APC accuracy report
- Fare count reports
- Route data exports

Dispatcher training overview

The planner training session provides in-depth instruction on the use of the Map Manager, Driver Messaging, and View Schedules module, as well as supporting system features that directly support the day-to-day operations between dispatch and drivers.

- What is an ITS system?
- What are the basic components of an ITS system?
- An introduction to the SPOT™ ITS
- General navigation
- Overview of system modules
- System configuration
- Map Module training
- Asset view
- Route view
- Vehicle information
- Stop information
- Assigning vehicles/drivers
- Alerts
- Off route
- No GPS
- In service/not in service
- Not tracking
- Asset grid
- View schedule module training
- Instant Replay module training
- Reports training
- Vehicle history (Breadcrumb)
- Vehicle set route/service
- OTP
- Arrival/departure
- Passenger counting
- Driver Messaging module training
- Putting it all together: The daily schedule performance
- Understanding how to validate data
- Working equipment
- Valid schedules
- Proper sign-in (system activity)
- Proper route execution
- Breadcrumbs
- Serviced stops and stop times
- Post-processing requests
- A day in the life of a dispatcher

Driver training overview

The driver training session provides in-depth instruction on the use of the mobile data terminal and information essential to the effective operation of vehicle-based systems.

- What is an ITS system?
- What are the basic components of an ITS system?
- Mobile data terminal (MDT) overview
- Power
- Connections
- Mounting
- MDT utilization
- Logging In
- Set route/service module training
- Fare Category module training (if equipped)
- Driver Messaging module training
- Driver Ops module training
- Electronic passenger counting training
- Announcements module training
- Digital manifest training (if equipped with demand-response)
- Anti-Bunching lock screen training (if equipped)

- On-time performance lock screen training (if equipped)
- System Status module training
- Load reset training
- Public website and app overview

Maintenance training overview

The maintenance training session provides in-depth instruction on the use of the various on-vehicle hardware components, including the MDT, vehicle logic unit, automatic passenger counters, audio systems, and other information essential to the effective troubleshooting and support of vehicle-based systems.

- What is an ITS system?
- What are the basic components of an ITS system?
- Mobile data terminal (MDT) overview
- Power
- Connections
- Mounting
- Onboard announcements overview
- Troubleshooting
- Automatic passenger counter overview
- Sensors and calibration
- Troubleshooting
- Interior signage overview
- Troubleshooting
- Head sign integration overview
- Troubleshooting

Planner training overview

The planner training session provides in-depth instruction on the use of the Route Manager module, as well as supporting system features that directly support the creation of new services, detours, announcements, blocks, and GTFS management.

- What is an ITS system?
- What are the basic components of an ITS system?
- An introduction to the SPOT™ ITS
- General navigation
- Overview of system modules
- System configuration
- Route Manager module training
- Import/export GTFS
- Creating and editing routes and patterns
- Creating and editing stops
- Creating and editing schedules
- Adding announcements
- Advanced announcements
- Adding destination codes
- Block builder
- Driver Messaging module training
- Instant Replay module training
- Route Planner module training
- Service Messages module training
- Station Manager module training
- User Manager module training
- System Configuration module training
- Map Module overview
- Reports Module overview
- Administrative tools
- Public Site Settings
- SPOT Console Settings
- Asset Configuration

Duration of training

ETA will consult with the City of Columbia on the scope and timing to develop a customized educational program designed around staff availability, roles, and specific areas of interest. In most cases, the SPOT™ training program takes around one week to adequately provide in-class and vehicle-based training.

Repetition is key

It is one thing to spend a day or two in a classroom learning about a system. It is another thing entirely to remember all the concepts and be able to immediately apply them one, two, or three days later in the performance of the job. It is not surprising then, to learn that the vast majority of 'issues' reported to technical support are not problems with the system itself, but rather a result of the performance of the people charged with using new equipment and software.

This is why ETA's training breaks up the training into two components: classroom and real-world, and uses our customer experience advocates to work alongside staff to make sure the information translates from conceptual to practical.

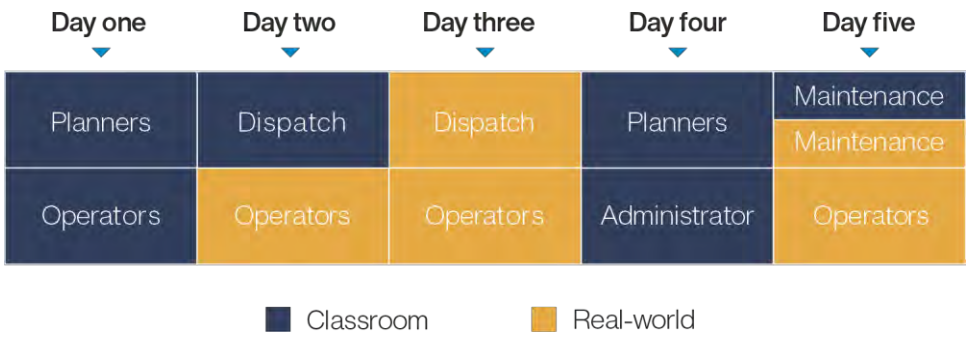


Figure 67: A sample instructional schedule based on a five-day training plan
ETA will work with your team to develop a right-sized curriculum for your situation.

The goal is to reinforce one day of classroom-based instruction that introduces concepts with real-world follow-up the very next day.

Day one: In two separate sessions, planners and operators are introduced to SPOT™ and key concepts.

- For planners, the goal is to create test routes within the SPOT™ Route Manager
- For operators, the goal is to understand their responsibilities within the system and become familiar with the mobile data terminal

Day two: In two separate sessions, dispatchers are introduced to SPOT and key concepts, while operators will put their day one lessons to good use by practicing on the test patterns created by the planners the day before.

- For dispatchers, the goal is to become comfortable with the Map and Driver Messaging modules
- For operators, the goal is to successfully log in to the MDT, assign a route/service, and run the test pattern correctly.

During this real-world training, operators will be shadowed by a customer experience advocate (CEA) who serves as a mentor and instructs on best practices. The CEA will also identify potential issues with routes for follow-up training with planners and ETA deployment team.

Day three: Dispatchers and operators work together on test routes

- For dispatchers, the goal is to build on comfort with the Map and Driver Messaging modules, work with information docks, and communicate changes to a service with the operator.
- For operators, the goal is building on prior-day successes and implement any changes communicated by dispatch.

During this real-world training, operators and dispatchers will be shadowed by a customer experience advocate (CEA) who serves as a mentor and instructs on best practices. The CEA will continue identify potential issues with routes for follow-up training with planners and ETA deployment team.

Day four: In separate sessions, planners are introduced to feedback from the prior two day of operator and dispatch training while administrators are exposed to the Reports module.

- For planners, the goal is review data collected by the routes they collected on day one and revise their test routes based on that feedback, plus that of operators and dispatch.
- For administrators, the goal is to run a series of reports based on actual data collected from the test routes.

During this real-world training, planners will be shadowed by a customer experience advocate (CEA) who serves as a mentor and instructs on best practices.

Day five: In separate sessions, maintenance is introduced to the SPOT™ ITS and connected systems, while operators go back on the road for additional training on test routes.

- For operators, the goal is continued proficiency and understanding of the MDT and to successfully implement changes made to routes by transit planners the day before.
- For maintenance teams, the goal is to achieve a high-level understanding of the SPOT™ ITS, its connected systems, and learn best practices for troubleshooting and servicing hardware.

During this real-world training, operators will be shadowed by a customer experience advocate (CEA) who serves as a mentor and instructs on best practices.

Supplemental training

Self-guided training and system instruction are available on ETA's online support portal, located at etatransit.force.com.

Key concept!

The training process is presented in an easy-to-follow manner and designed for non-technical learners. Each lesson dovetails into subsequent topics to create a logical and predictable instructional pathway.

GoCOMO responsibilities

We have kept this as simple as possible

As a provider of "turnkey" systems, ETA asks very little of our customers to implement the system. ETA will fulfill the lion's share of the implementation roles, including the scope of work found in the various sections defined elsewhere in the implementation strategy section.

To ensure a clean roll-out, we ask the City of Columbia to contribute to the following roles:

- Answer questions regarding customization, such as route configuration, schedules, and standard operating procedures
- Provide access to vehicles and maintenance staff at the time of installation
- Provide a meeting facility to train staff
- Provide custom graphics for traveler information systems (i.e., corporate colors, logos, etc.)
- Review and accept agency-specific field acceptance test procedures
- Participate in scheduled customer satisfaction calls
- Provide a clean file GTFS data for import and develop routes and geofencing in Route Manager

Warranty & support

[What you will discover]

ETA has a focused strategy for delivering an exceptional ownership experience from day one defined by a comprehensive warranty, sound support policies, and go-to-market campaign materials.

[Section key points]

- Warranty: By including a five year warranty and offering the option to extend coverage up to year nine, ETA Transit demonstrates their commitment to standing behind their product and providing GoCOMO with the necessary support for their hardware well into the future
- Support: The City of Columbia can expect to receive top-of-the-industry support from a dedicated team with clearly defined support procedures, ensuring efficient and comprehensive resolution of any issues that may arise
- Marketing: GoCOMO will benefit from a ready-made 'go-to-market' marketing campaign strategy, designed by an APTA Color Wheel Award winner, aimed at building anticipation and promoting adoption among staff and passengers, with full support provided

Feel supported!

"Perhaps more impressive was our after-market care. We still chat monthly about our changing situation and they make sure our capabilities meet the changing demands of our riders."

— Amy Seeboth, University of Wisconsin-Platteville

A 3-step approach

Our focus in providing you an incredible ownership experience

A critical component of the operational success of the SPOT™ platform is the care you receive after the sale and once the initial deployment is complete. ETA has dedicated itself to providing an exceptional tech ownership experience. This ongoing support consists of three components: a straightforward warranty clearly defined support procedures and the availability of go-to-launch marketing support materials.

1. Warranty overview

When you choose ETA as your transit partner, we want your experience to be as painless and efficient as possible. We underscore our commitment to providing an unparalleled ownership experience with the following key warranty promises:

- A 60-day guarantee on system installation
- A two-year warranty on ETA-installed system hardware and software for equipment failure and software issues as outlined within ETA's Service Level Agreement (SLA)
- Free software updates and patches for the life of the contract

Additionally, ETA provides an optional annual extended warranty through year five (5).

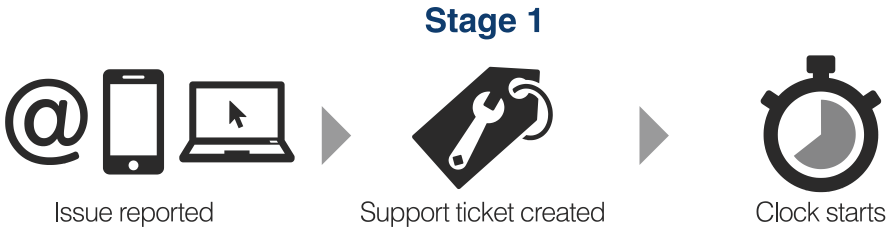
Coverage details:

- **Hardware**: Should ETA-installed equipment fail at any point during the warranty term of the agreement, we will replace it with a similar or equivalent product.
- **Software:** Any updates or upgrades to licensed ETA software will be immediately available for your application in your environment. This policy ensures you always have access to the latest technology releases and current software functionality.
- **Installation:** ETA guarantees the installation of its onboard system for sixty (60) days from vehicle acceptance. Should any defects in quality be discovered, we will assume the cost of remedy to the installation issue. This warranty does not cover the cost of any user-alterations or modifications to the initial installation.

2. Support overview

Should something not function as expected, ETA has developed a comprehensive information technology policy to help protect your investment, provide answers to your questions, and get your operations back on the road as quickly as possible. For a complete accounting of ETA support responsibilities, please refer to the Service Level Agreement located in Appendix C.

- **Maintenance and repair:** ETA will deliver peace-of-mind through the availability of an online reporting tool (etatransit.zendesk.com) to log any system issues you encounter. You tell us what difficulties you have encountered, and we will respond within one business day with a progress report in identifying the cause and present viable solutions. For urgent requests, please call us day or night at (561) 288-1932.
- **Disaster recovery:** Your configuration and route data are backed up off-site daily to nearby cloud-based servers. This feature ensures a continuation of care and safeguards to ensure that your critical data is protected and that recovery from a hardware error does not cost you precious time. Should something happen, we can restore data from other regional servers within moments.
- **Privacy policy:** Security is of paramount concern to ETA Transit. The data of our clients (and their clients) remains protected by up-to-date security practices, secure from outside entry. We never divulge confidential information to third parties, so the names, contact information, and system data remain safe and private, accessible only by those to whom you grant access. Visit etatransit.com/privacy to view our complete privacy policy.
- **Security:** Firewall ACLs protect ETA systems. We limit open ports to only those required for essential system operation with a quarterly rotation of all system passwords to enhance overall security.
- **Technical support and field repairs:** The ETA team understands that technical support, including a 24x7 toll-free technical support phone line, will be provided during the contract. The ETA team further understands that installation support, including licensing and software updates, will be provided during the contract. Issues that are not resolved by the level 1 prompt the technical support representative to escalate the problem to level 2 support. The ETA team is committed to assisting GoCOMO with fault diagnosis and repairs.



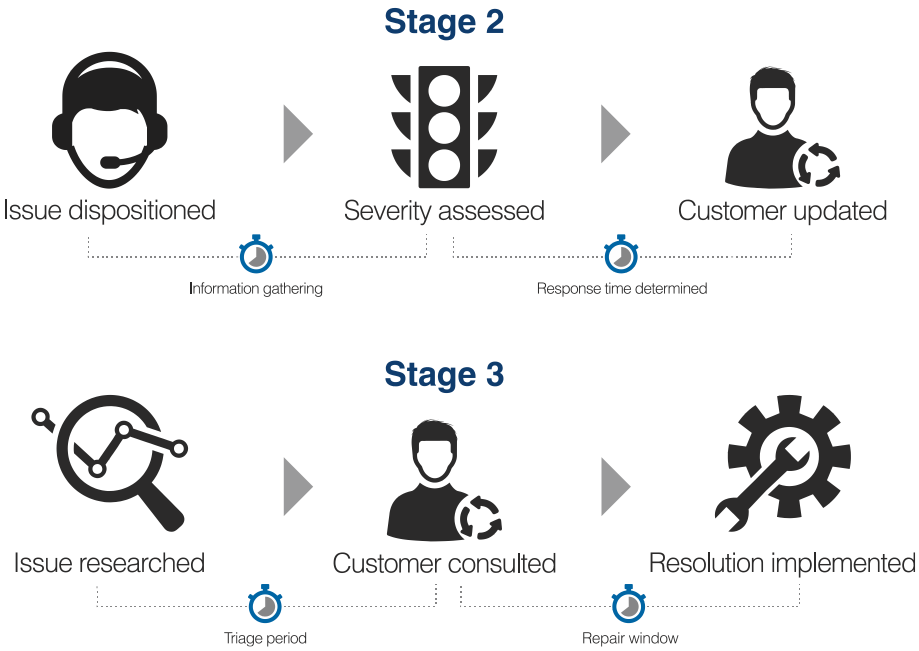


Figure 68: ETA's support process helps diagnose potential issues and defines achievable expectations for resolution.

Exclusions

ETA will always do everything possible to rectify every issue promptly. However, there are a few exclusions:

- Guarantees do not apply to software, equipment, or services not purchased or managed by ETA
- A problem is caused by using hardware, software, or service(s) in a manner outside of its intended function
- The client has made unauthorized changes to the configuration or setup of affected equipment, software, or service(s).
- The client has prevented ETA from performing required maintenance and update tasks
- An issue is related to unsupported equipment, software, or other services.
- The client is in breach of its contract with ETA for any reason (i.e., delinquent payment of fees)

3. Go-to-market support

Your new SPOT™ system is an investment in both infrastructure and rider satisfaction, and we have developed materials to reach out and build excitement among your staff and riders. We have

designed a complete go-to-market campaign to help you expand your outreach efforts. Ever mindful of your brand, our materials are be customized to reflect your market presence for little to no extra cost to you.

Our available go-to-market support materials include:

- Comprehensive, ready-made rollout marketing strategy
- Flyers and posters branded with your agency's logo and colors
- Tri-fold brochure
- Web banners
- Camera-ready print advertisements
- Website integration
- Social media campaigns with graphics and content
- Coloring and essay contests
- Links and QR codes to mobile apps (iOS and Android)

Figure 69: Sample materials include pre-launch web banners (top left), social media banners (top right), rider brochure (lower left), internal staff poster (center), and full-page newspaper print ad (lower right).

Appendices

[What you will discover]

The following appendices include additional information about ETA, its products, capabilities, and support that GoCOMO may find useful in its decision-making process.

[Section key points]

- **Reports:** A comprehensive listing of all available reports
- **Specifications:** Hardware specifications for key hardware components
- **Policies and procedures:** Corporate policies, including security and SLA documentation

What else can we discover?

The difference maker in this decision has been the dedication of the ETA Transit team in all phases of this project."

— Maureen Coughlin, Senior Facility Manager, SP+

Appendix A: Report listing

- Alerts Report
- Announcements
- APC Histogram by Station
- APC Pie Chart by Station
- APC Summary by Station
- Arrivals — Departures by Date
- Arrivals — Departures by Date (POST)
- Arrivals — Departures by Date (Run-Time)
- Audit Trips API
- Block Assignments
- Card Scan Histogram
- Card Scan Histogram by Station
- Card Scan Pie Chart
- Card Scan Pie Chart by Station
- Card Scan Summary
- Card Scan Summary by Station
- Card Scan Totals by Route
- Card Scan Totals by Stop
- Card Scan Totals by Vehicle
- Card Scans by Route-Stop
- Card Scans by Vehicle
- Cellular Outage by Date
- Cellular Outage by Route
- Cellular Outage by Vehicle
- Connectivity Summary
- Current Headways by Route
- Current Vehicle Assignments by Route
- Driver Assignment
- Driver Auth Attempts by Vehicle
- Driver Ops Details
- Drivers On-time Performance
- EPC by Route
- EPC by Route Chart
- EPC by Route Details
- EPC by Route-Stop
- EPC by Vehicle
- EPC by Vehicle Details
- Fare Count Histogram by Station
- Fare Count Passenger Summary
- Fare Count Pie Chart by Station
- Fare Count Ridership Report
- Fare Count Summary by Station
- Fare Counts by Vehicle
- Fuel Usage
- Fuel Usage by Day
- Fuel Usage by Driver
- Fuel Usage by Route
- Fuel Usage by Vehicle
- Geofence Trip Mileage
- GPS Outage by Date
- GPS Outage by Route
- GPS Outage by Vehicle
- Headsign Counts by Vehicle
- Headsign History Details
- Headsign History Summary
- Headway Summary Pie Chart
- Headways by Route
- Headways by Route and Station Group
- Headways by Route Group Threshold
- Headways by Stop
- Headways by Stop with Threshold
- Idle Time by Date
- MIT Accessory Details
- NTD Summary Report
- NTD Vehicle Operations
- On-time Performance

- On-time Performance — Monthly by Route
- On-time Performance — Monthly by Route-Stop
- On-time Performance Route- Stop
- Outage Details
- Passenger APC Histogram
- Passenger APC Pie Chart
- Passenger APC Summary
- Passenger Count by Trip
- Passenger Count Monthly Summary
- Passenger Count Monthly Summary Tabular
- Passenger Count Totals by Month
- Passenger Counts by Route, Stop, and Time Intervals
- Passenger Counts by Route-Details
- Passenger Counts by Route-Stop
- Passenger Counts by Vehicle-Details
- Passenger Counts by Vehicle-Doors
- Passenger Counts Per Route Summary
- Passenger Counts Vehicle Summary
- Passenger EPC Histogram
- Passenger EPC Pie Chart
- Passenger EPC Summary
- Passenger Fare Count Histogram
- Passenger Fare Count Pie Chart
- Passenger Fare Count Summary
- Passenger Load by Route
- Passengers by Route-Stop with Intervals
- PDS Connection Report
- Post Processing Audit Details
- Purged driver messages
- Report Hours and Mileage Summary
- Rider Feedback Report
- Ridership
- Ridership Totals by Type and Route
- Ridership With Fuel Info
- Route Manager Plan Details
- Scheduled Vehicle Miles and Hours
- Sign Health
- SMS Activity
- SMS Messages
- Stop Performance
- Unlinked Passenger Trips per Month
- Vehicle Assignment by Route
- Vehicle Deadhead Details
- Vehicle Engine Time Summary
- Vehicle Excessive Idle Time
- Vehicle History by ID
- Vehicle History by ID Tabular
- Vehicle Idle Time Summary
- Vehicle Mileage by Route
- Vehicle Mileage Summary
- Vehicle Number Assignment
- Vehicle Set Route
- Vehicle Speed Infractions
- Vehicle Speed Summary
- Vehicle Statistics by Trip
- Weekly Passenger Count Summary
- Wi-Fi Outage by Date
- Wi-Fi Outage by Route
- Wi-Fi Outage by Vehicle
- Yard Time And Mileage Report

Appendix B: Hardware specifications

Mobile data terminal

Technical details

- Screen size: 7” or 10.1” screen options
- Aspect ratio: 16:9
- Resolution: 1280x800 (native); 1920x1080 (maximum)
- Dimensions: 9.84375” X 6.6875” X 1.172” (250 mm X 170 mm X 29.6 mm)
- Weight: 2.52 lb (1144 g)
- Scan frequency: 60–72 Hz
- Response time: 20 ms
- Viewing angle: 140° x, 120° y (7”); 170° x, 170° y (10.1”)
- Brightness: 400 cd/m2 (7”); 350 cd/m2 (10.1”)
- Contrast ratio: 800:1
- LCD backlight: LED
- Video inputs: HDMI, VGA, Component, Composite, Audio outputs: <1.2W speaker, 3.5mm headphone output
- Touch screen inputs: Capacitive
- Input power: DC 12V
- Operating temp: -4° – 140°F / -20° – 60°C
- Mount type: VESA 75

Public address amplifier

Technical details

- Power: 10–30 volts DC
- Current consumption: Standby: 93mA; Max: 6A
- Dimensions: 8” x 3.125” x 1.75”; 203mm x 79mm x 44.5mm
- Weight: 1 lb 11 oz (0.76 kg)
- Load impedance: 4 – 8 Ohms
- Power output: 50 watts; 60 watts (max)
- Override: XLR priority microphone input overrides mini-fi t secondary microphone input
- Inputs: Dual microphone w/priority control; aux audio
- Volume: Internal speaker volume control

- Housing: Durable steel for easy installation
- Standard: Approved OEM standard option equipment

Vehicle logic unit

System

- CPU Intel® Gen4™ Dual Core 2980U 1.6 GHz
- Memory 1 x DDR3L-1600 SO-DIMM up to 8GB
- Graphics Intel® HD graphics
- ATA 2 x Serial ATA 2.0 ports with 6GB/s HDD transfer rate
- LAN chipset 2 x Intel i210-AT Gigabit Ethernet
- Watchdog 1 – 255 level resets

Inputs/outputs

- Serial port: Support 1 x RS-232 (COM1 with RS-232/422/485)
- USB port: 3 x USB 2.0 ports
- LAN: 2 x RJ45 ports for GbE
- Video port: 1 x HDMI and DVI-I
- GPIO port: Support 2 in and 2 out (12V / 100mA)
- Audio: Mic-in/Line-out
- Expansion bus: 3 x mini-card slots
- Antenna: 4 x SMA-type external antenna connectors for LTE/WLAN/UMTS/ GSM/GPRS/GPS/Bluetooth
- SIM card socket: 2 x SIM card sockets supported onboard with eject

Storage

- Type: 1 x 2.5” drive bay for SATA type hard disk drive/SSD

Qualification

- Certifications: CE, FCC Class A, eMark compliance

Software

- Operating system: Windows 7, WES 7, Windows 8.1, Linux 3.0.X

Power

- Power input: 9V–36V DC power input

- Power management: Vehicle power ignition for variety vehicle
- Power off control: Power off delay time setting by software (default is 5 minutes)
- Backup battery: Internal battery kit for 10 minutes (optional)

Environmental

- Operating temp.: -40°–70° C (SSD, ambient w/air)
- Storage temp.: -40°–80° C
- Relative humidity: 10%–90% (non-condensing)
- Vibration (random): 2.5g @ 5–500Hz with SSD
- Vibration (operating): MIL-STD-810F, method 516.5, category 20, ground vehicle-highway
- Truck storage: MIL-STD-810F, method 514.5, category 24, integrity test
- Shock Operating: MIL-STD-810F, method 516.5, procedure I, trucks, and semi-trailers=40G (11ms) with SSD
- Crash hazard: MIL-STD-810F, method 516.5, procedure V, ground equipment=100g

Mechanical

- Construction: Aluminum allow
- Mounting: Wall-mount, VESA mount, DIN rail mounting kit
- Weight: 1406g
- Dimensions: 182 mm x 167.6 mm x 52 mm

Appendix C: Sample SLA

Service Level Agreement

Parties

This System Warranty and Support Agreement ("Agreement") is made on this _____ day of_____, 20_____ (the execution date) between ETA Phi Systems, Inc. ("ETA") having an office at 7700 Congress Ave., Suite 2201, Boca Raton, FL, 33487 and _____ ("Customer") having an office at _____.

ETA contact:

Name: Nicole Castonguay

Title: CEO

Telephone: 719-453-0251

Email: ncastonguay@etatransit.com

Customer contact:

Name: _____

Title: _____

Telephone: _____

Email: _____

Overview

WHEREAS Customer and ETA entered into an agreement for the purchase of hardware, software, and related services on the execution date; and

WHEREAS Customer desires to obtain support services for said hardware and software (collectively "System"); and

WHEREAS ETA desires to provide such support services.

Now therefore, the parties, for good and valuable consideration, agree to the following

1. Hardware warranty and support

1.1 Hardware products

The hardware products covered by this agreement shall be as set forth on the included in the Quotation or Purchase Order attached as Exhibit 1. If the quantity of products changes during the term of this agreement, a corresponding adjustment to fees hereunder will apply for the remaining term of the agreement.

Consumable Items such as batteries, cables, wiring harnesses, GPS, WLAN and RF antennas, etc. are not covered under this agreement. Replacements for such items may be ordered from ETA and will be subject to the supplier's warranty policy.

1.2 Hardware warranty

ETA affirms that each hardware product is free of defects in material and workmanship. ETA further affirms that hardware products will perform for the intended purpose for a period of two (2) years from delivery of equipment. Thereafter, the provisions under Non-Warranty Repairs shall apply. For Contracts that are shorter than two (2) years in length, the hardware warranty shall not exceed the term of the Contract. Extended warranties can be quoted upon request for up to a total of five (5) years of warranty.

1.3 Warranty repair policy

If a hardware product fails to operate as specified, and no exclusions from warranty policy apply, ETA or its authorized service agents will have the option to repair or replace the defective product at no cost to the Customer.

1.4 Exclusions from warranty policy

Instances to which the Warranty Repair Policy shall not apply include, but are not limited to; a) warranty returns classified as No Problem Detected (determined to be fully functional with no need for repair), b) product failures resulting from improper use, c) damage resulting from accident, abuse or improper maintenance, d) damage caused by operation outside ETA specifications, e) damage resulting from vandalism, fire, or other uncovered peril, e) product modified without ETA's consultation, and f) Consumable Items.

In such instances, the provisions under Non-Warranty Repairs, including applicable fees, shall apply.

1.5 Warranty service

1.5.1 Spare parts inventory

The Customer shall maintain an inventory of ETA hardware products at the recommended level for use during completion of repairs. The Customer is responsible to; remove defective products, replace them with spare products, request Return Material Authorization ("RMA") number, and to send defective products to ETA for Failure Analysis.

1.5.1.1 Return material authorization

No product received for repair by ETA will be accepted without an ETA-assigned RMA number. RMA numbers may be obtained by:

Phone: 561-288-1932
Email: support@etatransit.com
ZenDesk System Access: etatransit.zendesk.com

RMA requests shall include product description, ETA part number, serial number (if applicable), quantity, reason for return, and vehicle number (if applicable). The Customer is responsible to ensure secure packaging of products for shipping. Shipping material is available for purchase, at cost, from ETA. ETA is not responsible for damage to, or loss of, products in transit. Shipping costs for the return to ETA of products to which the Warranty Repair Policy applies will be borne by ETA. Shipping costs for the return to ETA of products deemed Exclusions of Warranty Policy will be borne by the Customer. Customer agrees to ship RMAs using an ETA-supplied shipping label. RMA shipments are to be labeled as follows:

ETA Transit Systems, Inc.
Attn: Customer Service, RMA #_____
7700 Congress Ave, Suite 2201
Boca Raton, FL 33487

1.5.1.2 Failure analysis and repair/replace

Upon receipt of a returned product, an ETA technician will complete a failure analysis to decide of whether the product is subject to the Warranty Policy or the Exclusions of Warranty Policy, and whether to product is repairable. If the product is subject to the Warranty Policy ETA will either repair or replace the product at ETA's discretion. If the product is subject to the Exclusions of Warranty Policy ETA will provide the Customer a quotation and subsequent invoice for the repair or replacement of the product.

1.5.1.3 Return

ETA will make its best effort to return the repaired or replaced product to the Customer within thirty (30) days. Shipping costs for the return to Customer of repaired or replaced products to which the Warranty Repair Policy applies will be borne by ETA. Shipping costs for the return to Customer of repaired or replaced products deemed Exclusions of Warranty Policy will be borne by the Customer.

1.6 Non-warranty repairs

Repairs of products performed by ETA which are Exclusions of Warranty Policy, or otherwise not covered by the Warranty Repair Policy, will be invoiced to the Customer at the applicable Bench Rate, for repairs performed at ETA facilities, and/or Field Service Rate below, along with other time and material costs incurred by ETA. The Warranty Repair Policy will apply to non-warranty repairs for a period of ninety (90) days from shipment to Customer.

1.7 Hardware support rates

ETA quotations and/or invoices for Non-Warranty Repairs shall include any combination of the following that may apply:

Bench rate: $125/hr., one (1) hour minimum, charged to the nearest ½ hr.

Field service rate: $150/hr., charged to nearest 1/2 hr., applies to actual time at customer facility as well as round trip travel time.

Travel & miscellaneous: Actual cost of commercial coach airfare, rail, bus, rental car, taxis, tolls, parking incurred (and supported by receipts)

Mileage: Current IRS allowance rate/mile

Meals: Current federal government regional per-diem rate

1.8 Customer hardware maintenance obligations

In addition to the responsibilities identified in this Section 5, the Customer shall:

- Provide access to vehicles and maintenance staff at time of installation
- Review and accept agency-specific design documentation and acceptance test procedures
- Participate in scheduled project status and customer satisfaction calls
- Pay all invoices according to the applicable payment terms
- Provide reasonable access to the Customer's facilities, vehicles and systems required for ETA to perform required tasks (subject to Customer's security requirements)
- Provide technical and administrative support to ETA's on-site personnel (office supplies, photocopying, network access, etc.)
- Faithfully execute required maintenance and troubleshooting procedures as prescribed by ETA.

2. Software maintenance and support

2.1 Software products

The software products covered by this agreement shall be as set forth in included in the Quotation or Purchase Order attached as Exhibit 1. If the quantity of products changes during the term of this agreement, a corresponding adjustment to fees hereunder will apply for the remaining term of the agreement. Provisions hereunder are subject to the Software Subscription Agreement attached as Exhibit 2, and no provision hereunder will apply to software not licensed by the Customer under a Software Subscription Agreement with ETA.

2.2 Software maintenance and support services

During the term ETA agrees to provide certain services in support of the Customer's use of the licensed software products. Services shall consist of:

- Provide Technical Support Help Desk – see Section 8 – System Warranty and Support
- Provide Software Updates – Modifications or additions to software product that bring the product into conformity with stated specifications, including correction of errors or bugs.
- Provide Software Maintenance – Activities performed to ensure software product performs in conformity with stated specifications.
- Provide Software Upgrades – Improvements, feature additions or other enhancements which are in addition to stated specifications.

2.3 Additional software services

Services performed by ETA in response to the following, are excluded from Software Maintenance and Support Services and will be quoted and invoiced to the Customer at the applicable Software Developer Rate, for activities performed at ETA facilities, and/or Field Service Rate below, along with other time and material costs incurred by ETA:

- Customer request for Update or Upgrade Installation Labor
- Customer request for Enhancements
- Customer request for Integration with third party software or hardware that are not included in the Quotation or Purchase Order attached as Exhibit 1
- Problems resulting from the hardware on which the software product is installed, or problems resulting from hardware devices connected to the hardware on which the software product is installed
- Problems resulting from the misuse, alteration, or damage of the software product
- Problems resulting from Customer use of versions of the software product other than the most recent update delivered by ETA

2.4 Software service rates

ETA quotations and/or invoices for Additional Software Services shall include any combination of the following that may apply:

- **Software developer rate:** $150/hr., one (1) hour minimum, charged to the nearest half hour
- **Senior software developer rate:** $175/hr., one (1) hour minimum, charged to the nearest half hour
- **Systems architect rate:** $250/hr., one (1) hour minimum, charged to the nearest half hour
- **Field service rate:** $150/hr., charged to nearest half hr., applies to actual time at Customer facility as well as round trip travel time
- **Travel & miscellaneous:** Actual cost of commercial coach airfare, rail, bus, rental car, taxis, tolls, parking incurred (and supported by receipts)
- **Mileage:** Current IRS allowance rate/mile
- **Meals:** Current federal government regional per-diem rate

2.5 Remote software access

As the software products, as well as relevant Customer data, are hosted by ETA in an internet-accessible environment, both Customer and ETA access is critical to the performance of

Software Maintenance and Support Services and Additional Software Services hereunder. Both parties agree to:

- Take all reasonable steps to facilitate timely access to required software instances and data by the other party
- Take all reasonable steps to avoid disruption of other operations of the other party
- Abide by the other party's IT security policies
- Refrain from accessing any internal or internet-based networks of the other party for purposes other than performance hereunder.

3. System warranty and support

3.1 System warranties (other than hardware and software product warranties)

3.1.1 Installation

ETA guarantees the installation of its Hardware and Software products for a period of 60 days commencing at the Installation Milestone. Should any defects be discovered, ETA will assume the cost to remedy the installation issue. This guarantee excludes any alterations or modifications to the initial installation made by the Customer.

3.1.2 Security

ETA hosted systems are protected by firewall Access Control Lists. Open ports shall be limited to those required for Customer operation, and a quarterly rotation of login credentials deployed for secure operations. Please refer to the ETA Transit Systems Information Technology Security Policy for further details.

3.1.3 Privacy

Customer data and other confidential information of Customer shall be maintained in such a manner as to prevent access by any party other than ETA and Customer-designated personnel.

3.1.4 Disaster recovery

ETA shall perform daily backups of Customer data to regional cloud-based servers. Restorations of backups will be performed at no incremental cost to Customer and will be completed within 8 hours of request.

3.1.5 Annual maintenance

At ETA's discretion, ETA may execute an annual onsite visit to Customer premises to perform visual inspections. Repairs deemed critical to the operation of the system may be performed at ETA's discretion. Recommendations and associated quotations for replacements, upgrades or improvements will be provided within 30 days after such annual maintenance onsite visit.

3.1.6 Ongoing system support

ETA provides System Support 7 days per week, 365 days per year (24x7x365), via; online helpdesk/ticket monitoring system (ZenDesk), and dedicated email addresses. Live chat is available between the hours of 8AM and 5 PM Monday through Friday, Eastern Standard Time. Telephone support outside of ETA's normal business hours, 8AM and 5 PM Monday through Friday, Eastern Standard Time is reserved for emergencies.

ETA shall maintain technical personnel qualified to perform the tasks of; logging support tickets, responding to Customer RMA requests, severity determination, issue resolution, onsite issue resolution. ETA has sole discretion over the deployment of resources required to perform these tasks, whether a task is required, and whether a task is covered by warranty.

3.2 System support process

The parties acknowledge their respective obligations associated with the following steps associated with submitting, acknowledging, researching, and resolving problems and requests. The timelines for these steps are dictated by the Problem Severity and Resolution framework under Section 5.3.

- **Stage 1** – Customer notifies ETA of an issue via one of the three accepted methods, ETA logs support ticket and acknowledges receipt to Customer

- **Stage 2** – ETA reviews issues, Customer provides timely response to any requested clarifications, ETA determines severity, ETA informs Customer of severity level
- **Stage 3** – ETA will research issue resolution and estimate resolution time estimate, ETA consults with customer on resolution and time estimate, Customer responds in a timely manner, ETA implements resolution and informs Customer of issue-closure

3.3 Problem severity, response, and resolution

Pursuant to ETA's System Support Process, ETA personnel shall decide of the severity of all issues received by Customer. While response times are committed for each severity, the issue resolution time shall be on a case-specific basis, independent of severity level. Once resolution times are estimated, the penalty to ETA of exceeding the estimated resolution time shall vary based on severity. Severity definitions, response times and penalties for exceeding resolution times are as follows:

Severity Level	Description (including examples)
Fatal	Complete system failure
Severe	A majority of system functionality is impacted
Medium	A minority of system functionality is impacted

Severity Level	Response Time	Resolution Time	Penalty per Hour
Fatal	30 minutes (*)	Case-specific	3% total monthly fee
Severe	4 hours	Case-specific	2% total monthly fee
Medium	8 hours	Case-specific	1% total monthly fee

3.4 Service level commitment and penalties

The parties acknowledge that the System is a complex technical solution, the effective operational uptime of which is dependent on the interaction between hardware, software, vehicles, and various user and support personnel of both ETA and the Customer. The parties agree to make all reasonable efforts to minimize downtime of the overall System, the functionality of the System and any vehicles on which the System is installed. Accordingly, ETA shall incur penalties for operational downtime, according to the severity of the issues defined under Section 5.3. This instance may trigger penalties; Cumulative downtime for a severity level for a month exceeds the allowable levels below.

Severity Level	Allowable Downtime/Month	Penalty per Hour
Fatal	2 hours	3% total monthly fee
Severe	8 hours	2% total monthly fee
Medium	20 hours	1% total monthly fee

Penalties shall take the form of credits which the Customer may apply against existing and future ETA invoices. A cumulative maximum of 25% of total monthly fees shall apply.

3.5 Customer system maintenance obligations

In addition to the responsibilities identified in this Section 5, the Customer shall:

- Answer questions regarding customization, such as route configuration, schedules, and standard operating procedures
- Provide a meeting facility to train staff
- Provide custom graphics for traveler information systems (i.e. corporate colors, logos, etc.)
- Review and accept agency-specific design documentation and acceptance test procedures
- Participate in scheduled project status and customer satisfaction calls
- Pay all invoices according to the applicable payment terms
- Provide 24-hour access to the Customer's facilities, vehicles and systems required for ETA to perform required tasks (subject to Customer's security requirements)
- Provide technical and administrative support to ETA's on-site personnel (office supplies, photocopying, network access, etc.)

4. General provisions

4.1 Intellectual property

4.1.1 Retention of ETA rights in hardware products

All proprietary and intellectual property rights, including copyrights or trademarks in the Hardware Products, if any, and any modifications thereto shall remain the sole and exclusive property of ETA.

4.1.2 Retention of ETA rights in software products

As between ETA and Licensee, all proprietary and intellectual property rights, title and interest in the Software Products and any Updates, Upgrades, and any other modification to the Software Products and associated documentation shall be and remain the sole and exclusive property of ETA. The Licensee has no proprietary or intellectual property rights

title or interest in the Software Products or any Updates, Upgrades, or any modification to the Software Products or associated documentation. Unless ordered by a court of jurisdiction, Licensee not at any time disclose, furnish or make available to anyone the source and executable code of the software or related documentation or other confidential information of ETA. Licensee's use of the Software Products and any Updates, Upgrades, and any other modification to the Software Products and associated documentation shall be subject to the terms and conditions of the Software Subscription Agreement attached as Exhibit 2.

4.2 Authority

The parties to this Agreement warrant and represent that they have the power and authority to enter into this Agreement in the names and capacities stated herein.

ETA and Customer hereby agree to the provisions of this Agreement:

ETA PHI Systems, Inc.:

By: _____

Name: _____

Title: _____

Customer:

By: _____

Name: _____

Title: _____

Appendix D: Open-source software

Comprehensive listing of all OSS or third-party code

Software name	License type	Link to license (if provided)
highcharts	GPL 3.0 (Commercial)	Can provide if requested
jscolor	GPL 3.0 (Commercial)	Can provide if requested
select2	MIT	https://github.com/select2/select2/blob/master/license.md
dropzone	MIT	Inline
filesaver	MIT	https://github.com/eligrey/filesaver.js/blob/master/license.md
markerclusterer	Apache 2.0	http://www.apache.org/licenses/license-2.0
flatpickr	MIT	https://github.com/flatpickr/flatpickr/blob/master/license.md
html2canvas	MIT	Inline
enquire	MIT	http://www.opensource.org/licenses/mit-license.php
respond	MIT	Inline
loader	Apache 2.0	Inline
date	MIT	http://www.datejs.com/license/
tinycolor	MIT	https://github.com/bgrins/tinycolor/blob/master/license
canjs	MIT	Inline
jqueryui	MIT	Inline
jquery	MIT	https://github.com/jquery/jquery/blob/master/license.txt
jquery-impromptu	MIT	Inline
jquery-scrolltofixed	MIT	https://github.com/bigspotteddog/scrolltofixed/blob/master/license.txt
jquery-dragtable	MIT	Inline
jquery.jcrop	MIT	https://github.com/tapmodo/jcrop/blob/master/mit-license.txt
jquery.simplcropper	MIT	https://github.com/tomazdragar/simplecropper/blob/master/license
jquery.ui.touch-punch	MIT	Inline

Software name	License type	Link to license (if provided)
jquery.dataTables	MIT	http://datatables.net/license
jquery.stupidtable	MIT	https://github.com/joequery/stupid-table-plugin/blob/master/license
jquery-masked-input	MIT	http://digitalbush.com/projects/masked-input-plugin/#license
socket.io	MIT	https://github.com/socketio/socket.io/blob/master/license
bootstrap	MIT	https://github.com/twbs/bootstrap/blob/main/license
bootstrap-confirmation	Apache 2.0	Inline
bootstrap-datepicker	Apache 2.0	http://www.apache.org/licenses/license-2.0
bootstrap-timepicker	MIT	https://github.com/jdewit/bootstrap-timepicker/blob/gh-pages/license
bootstrap-datetimepicker	MIT	https://github.com/jdewit/bootstrap-timepicker/blob/gh-pages/license
bootstrap-multiselect	Apache 2.0	https://github.com/davidstutz/bootstrap-multiselect/blob/master/license.md
bootstrap-colorpicker	MIT	https://github.com/itsjavi/bootstrap-colorpicker/blob/master/license
event	MIT	Inline
dual-listbox	MIT	https://github.com/maykinmedia/dual-listbox/blob/master/license
jszip	MIT	https://github.com/nodeca/pako/blob/master/license
ejs	Apache 2.0	https://github.com/mde/ejs/blob/main/license
context	MIT	Inline
remodal	MIT	https://github.com/vodkabears/remodal/blob/master/license
sortable	MIT	Inline
fontawesome	CC/MIT	https://fontawesome.com/license/free

Appendix E: IT security policy

Introduction

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement to ensure the integrity and availability of the data environment at ETA Transit Inc., hereinafter, referred to as the **Company**. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Company with policies and guidelines concerning the acceptable use of Company technology equipment, e-mail, Internet connections, voicemail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Company employees or temporary workers at all locations and by contractors working with the Company as subcontractors.

Scope

This policy document defines common security requirements for all Company personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Company, entities in the private sector, in cases where Company has a legal, contractual, or fiduciary duty to protect said resources while in Company custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Company network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Company in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Company domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Company at its office locations or at remote locales.

Acronyms/definitions

Common terms and acronyms that may be used throughout this document.

CEO:

The Chief Executive Officer is responsible for the overall privacy and security practice of the company.

CTO:

The Chief Technology Officer

CO:

The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues.

CST:

Confidentiality and Security Team

DoD:

Department of Defense

Encryption:

The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'

External media:

CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

File Allocation Table (FAT):

The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted, and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

Firewall:

A dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

FTP:

File Transfer Protocol

IT:

Information technology

Local Area Network (LAN):

A computer network that covers a small geographic area, i.e. a group of buildings, an office.

New Technology File Systems (NTFS):

NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

Statement of Work (SOW):

An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

User:

Any person authorized to access an information resource.

Privileged Users:

System administrators and others specifically identified and authorized by Company management.

Users with edit/update capabilities:

Individuals who are permitted, based on job assignment, to add, delete, or change records in a database.

Users with inquiry (read only) capabilities:

Individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

VLAN:

Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

Virtual Private network (VPN):

Provides a secure passage through the public Internet.

Wide Area Network (WAN):

A computer network that enables communication across a broad area, i.e. regional, national.

Virus:

A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

Employee responsibilities

Employee requirements

The first line of defense in data security is the individual Company user. Company users are responsible for the security of all data which may come to them in whatever format. The Company is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear identifying badge so that it may be easily viewed by others. In order to help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in Company facilities are provided with a contactor badge as well. Other people who may be within Company facilities should be wearing visitor badges and should be chaperoned.

Challenge unrecognized personnel. It is the responsibility of all Company personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Company office location, you should challenge them as to their right to be there. All visitors to Company offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the Company. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure laptop with a cable lock. When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers. Most Company computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof but do provide an additional level of security. Many

laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all the equipment he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended computers. Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Company policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home use of company corporate assets. Only computer hardware and software owned by and installed by the Company is permitted to be connected to or installed on Company equipment. Only software that has been approved for corporate use by the Company may be installed on Company equipment. Personal computers supplied by the Company are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Company for home use.

Retention of ownership. All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Company are the property of the Company unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Company employees at their own expense.

Prohibited activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- **Crashing an information system.** Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred because of user action, a repetition of the action by that user may be viewed as a deliberate act.
- **Attempting to break into an information resource or to bypass a security feature.** This includes running password-cracking programs or sniffer programs and attempting to circumvent file or other resource permissions.
- **Introducing, or attempting to introduce, computer viruses, trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.**

- **Exception:** Authorized information system support personnel, or others authorized by the Company Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

- **Browsing.** The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- **Personal or unauthorized software.** Use of personal software is prohibited. All software installed on Company computers must be approved by the Company.
- **Software use.** Violating or attempting to violate the terms of use or license agreement of any software product used by the Company is strictly prohibited.
- **System use.** Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Company is strictly prohibited.

Electronic communication, e-mail, Internet usage

As a productivity enhancement tool, The Company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Company owned equipment are considered the property of the Company – not the property of individual users. Consequently, this policy applies to all Company employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Company provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible so long as:

1. It does not consume more than a trivial amount of employee time or resources,
2. It does not interfere with staff productivity,
3. It does not preempt any business activity,
4. It does not violate any of the following:

a. **Copyright violations.** This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

b. **Illegal activities**. Use of Company information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.

c. **Commercial use.** Use of Company information resources for personal or commercial profit is strictly prohibited.

d. **Political activities.** All political activities are strictly prohibited on Company premises. The Company encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.

e. **Harassment**. The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Company prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include but is not limited to: ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f. **Junk e-mail.** All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the Company's equipment,

networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Company reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Company policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

Internet access

Internet access is provided for Company users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Company should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the Company routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

Reporting software malfunctions

Users should inform the appropriate Company personnel when the user's software does not appear to be functioning correctly. The malfunction—whether accidental or deliberate—may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Company computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or Company IT administrator as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The IT administrator should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

Report security incidents

It is the responsibility of each Company employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Company CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Company CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the

remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Company Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of sensitive/confidential information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Company and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Company policy and will result in personnel action and may result in legal action.

Transferring software and files between home and work

Personal software shall not be used on Company computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Company purchased software on home or on non-Company computers or equipment.

Company proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the Company without written consent of the respective supervisor or department head. It is crucial to the Company to protect all data and, to do that effectively we must control the systems in which it is contained. If a supervisor or department head receives a request to transfer Company data to a non-Company computer system, the supervisor or department head should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

The Company Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the Company does not control non-Company personal computers, the Company cannot be sure of the methods that may or may not be in place to protect Company sensitive information, hence the need for this restriction.

Internet considerations

Special precautions are required to block Internet (public) access to Company information resources not intended for public access, and to protect confidential Company information when it is to be transmitted over the Internet. The following security and administration issues shall govern Internet usage.

Prior approval of the Company Privacy Officer or appropriate personnel authorized by the Company shall be obtained before:

- An Internet, or other external network connection, is established
- Company information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g., web or ftp server) or device
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor
- Use shall be consistent with the goals of the Company. The network can be used to market services related to the Company, however, use of the network for personal profit or gain is prohibited
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet
- The encryption software used, and the specific encryption keys (e.g., passwords, pass phrases), shall be escrowed with the Company Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Identification and authentication

User logon IDs

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are audited at least twice yearly, and all inactive logon IDs are revoked. The Company Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Passwords

User account passwords

User IDs and passwords are required to gain access to all Company networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length. Passwords are required to be a minimum of eight characters.

Content Requirements. Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency. Passwords must be changed every 90 days. Compromised passwords shall be changed immediately.

Reuse. The previous twelve passwords cannot be reused.

Restrictions on Sharing Passwords. Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords. Passwords are masked or suppressed on all online screens and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

Confidentiality agreement

Users of Company information resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the Company information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Company information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending, or employees are leaving an organization.

Access control

Information resources are protected using access control systems. Access control systems include both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Request Form. This form can only be initiated by the appropriate department head and must be signed by the department head and the Security Officer or appropriate personnel.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

Termination of user logon account

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the IT Department of employee's last scheduled workday so that their user account(s) can be configured to expire. The employee's department head shall be responsible for ensuring that all keys, ID badges, and other access devices as well as Company equipment and property is returned to the Company prior to the employee leaving the Company on their final day of employment.

No less than quarterly, the IT Manager or their designee shall provide a list of active user accounts for both network and application access, to department heads for review. Department heads shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by the Company, the department head will immediately notify the IT Department of the employee's termination.

Network connectivity

Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of ETA Transit, LLC policy, we must mitigate these external risks the best of our ability.

Purpose

The purpose of this policy is to define rules and requirements for connecting to Company network from any host. These rules and requirements are designed to minimize the potential exposure to Company from damages which may result from unauthorized use of Company resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Company internal systems, and fines or other financial liabilities incurred because of those losses.

Scope

This policy applies to all Company employees, contractors, vendors and agents with a Company owned or personally owned computer or workstation used to connect to the Company network. This policy applies to remote access connections used to do work on behalf of Company, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to Company networks.

Policy

It is the responsibility of Company employees, contractors, vendors and agents with remote access privileges to Company's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Company

General access to the Internet for recreational use through the Company network is strictly limited to Company employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Company network from a personal computer, Authorized Users are responsible for preventing access to any Company computer resources or data by non-Authorized Users. Performance of illegal activities through the Company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Company networks to access the Internet for outside business interests.

For additional information regarding Company's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website.

Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.
- Authorized Users shall protect their login and password, even from family members.
- While using a Company-owned computer to remotely connect to Company's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct Company business must be approved in advance by InfoSec and the appropriate business unit manager.
- All hosts that are connected to Company internal networks via remote access technologies must use the most up-to-date anti-virus, this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

Malicious code

Antivirus software installation

Antivirus software is installed on all Company personal computers and servers. Virus update patterns are updated daily on the Company servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Remote Deployment Configuration. Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting. A record of virus patterns for all workstations and servers on the Company network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

New software distribution

Only software created by Company application staff, if applicable, or software approved appropriate personnel will be used on internal computers and networks. All new software will be tested by appropriate personnel to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Company computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage Company hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Company computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Company personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device are a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Company computer or network.

Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer

when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not “bootable”.

Retention of ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Company are the property of the Company unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Company ownership at the time of employment. Nothing contained herein applies to software purchased by Company employees at their own expense.

Acceptable use policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Company. These rules are in place to protect the employee and Company. Inappropriate use exposes Company to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Company business or interact with internal networks and business systems, whether owned or leased by Company, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Company policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Company.

Policy

General use and ownership

- Company proprietary information stored on electronic and computing devices whether owned or leased by Company, the employee or a third party, remains the sole property of Company. You

must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

- You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Company proprietary information.
- You may access, use or share Company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Company may monitor equipment, systems, and network traffic at any time, per Infosec's *Audit Policy*.
- Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and proprietary information

- All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
- System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Company, unless posting is during business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Company-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and network activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Company.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Company or the end user does not have an active license is strictly prohibited.
- Accessing data, a server, or an account for any purpose other than conducting Company business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Company account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.

- Introducing honeypots, honeynets, or similar technology on the Company network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Company employees to parties outside Company.

Email and communication activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Company or connected via Company's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and social media

- Blogging by employees, whether using Company’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Company’s systems to engage in blogging is acceptable, if it is done in a professional and responsible manner, does not otherwise violate Company’s policy, is not detrimental to Company’s best interests, and does not interfere with an employee's regular work duties. Blogging from Company’s systems is also subject to monitoring.
- Company’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or

any other material covered by <Company>'s Confidential Information policy when engaged in blogging.

- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Company and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Company's *Non-Discrimination and Anti-Harassment* policy.
- Employees may also not attribute personal statements, opinions or beliefs to Company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Company. Employees assume all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Company's trademarks, logos, and any other Company intellectual property may also not be used in connection with any blogging activity

Encryption

Definition

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

Encryption key

An encryption key specifies the transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Company shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. The Company employs several methods of secure data transmission.

Use of WinZip encrypted and zipped e-mail

This software allows Company personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Company staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites using appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

Secure Socket Layer (SSL) web interface

Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website.

Building Security

It is the policy of the Company to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Company strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the Company. All other facilities, if applicable, have similar security appropriate for that location.

- Entrance to the building during non-working hours is controlled by a security badge system. Attempted entrance without a badge results in immediate notification to the police department.
- Only specific Company employees are given the keys for the entrance. Giving the keys to non-employees is strictly prohibited.
- The door to the reception area is always locked and requires appropriate badges.
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk and should be accompanied by a Company staff member. In some situations, non-Company personnel, who have signed the confidentiality agreement, do always not need to be accompanied.
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Company considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Company office environment. It applies to users who work from their home full time to employees on temporary travel, to users who work from a remote office location, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Company's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

General requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to know.** Telecommuting users will have the access based on the same 'need to know' as they have when in the office.
- **Password use.** The use of a strong password, changed at least every 90 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training.** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract specific.** There may be additional requirements specific to the individual contracts to which an employee is assigned.

Hardware Security Protections

Virus protection. Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Company personal computers and is set to update the virus pattern daily. This update is critical to the security of all data and must be allowed to complete.

VPN and firewall use. Established procedures must be rigidly followed when accessing Company information of any type. The Company requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Security locks. Always use security cable locks for laptops, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock screens. No matter what location always lock the screen before walking away from the workstation. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

Data security protection

Data backup. Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established, or if you have external media that is not encrypted, contact the appropriate Company personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring data to the Company. Transferring of data to the Company requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Company.

External system access. If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail. Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Company networks. Extreme care must be taken when connecting Company equipment to a home or hotel network. Although the Company actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Company has no ability to monitor or control the security procedures on non-Company networks.

Protect data in your possession. View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted workspaces. If your laptop has not been set up with an encrypted workspace, contact the appropriate personnel for assistance.

Hard copy reports or work papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data entry when in a public location. Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e., airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending data outside the company. All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside the Company without the written approval of your supervisor.

Disposal of paper and/or external media

Shredding. All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Company work environment, MUST have direct access to a shredder.

Disposal of Electronic Media. All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The appropriate personnel have very definitive procedures for doing this – so all external media must be sent to them.
- The last step in this process is to forward the media for disposal by a certified destruction agency.

Specific protocols and devices

Wireless usage standards and policy

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Company employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Company laptops and mobile devices.

Approval Procedure. To be granted the ability to utilize the wireless network interface on your Company laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the appropriate personnel of the Company. Once this form is completed and approved you will be contacted by appropriate Company personnel to setup your laptop and schedule training.

Software requirements. The following is a list of minimum software requirements for any Company laptop that is granted the privilege to use wireless access:

- Windows XP with Service Pack 3 (firewall enabled)
- Antivirus software
- Appropriate VPN Client, if applicable
- Internet Explorer 6.0 SP2 or Greater

If your laptop does not have all these software components, please notify your supervisor or department head so these components can be installed.

Training requirements. Once you have gained approval for wireless access on your Company computer, you will be required to attend a usage and security training session to be provided by the appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted, and in most cases will include several individuals at once.

Use of transportable media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Company in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Company networks. Every workstation or server that has been used by either Company employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore, procedures must be carefully followed when copying data to or from transportable media to protect sensitive Company data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a Company employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common practice within the Company. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Company networks. Transportable media received from an external source could potentially pose a threat to Company networks. ***Sensitive data*** includes all human resource data, financial data, Company proprietary information.

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much-improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No **sensitive data** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Company data or sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Company.
- Non-Company workstations and laptops may not have the same security protection standards required by the Company, and accordingly virus patterns could potentially be transferred from the non-Company device to the media and then back to the Company workstation.
- Data may be exchanged between Company workstations/networks and workstations used within the Company. The very nature of data exchange requires that under certain situations data be exchanged in this manner.
- It is permissible to connect transferable media from other businesses or individuals into Company workstations or servers as long as the source of the media in on the Company Approved Vendor list.
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves the Company, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

The Company utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Company laptops, workstation, or servers must be wiped of data in a manner. All transportable media must be wiped according to the same standards. Thus, all transportable media must be returned to the appropriate personnel for data erasure when no longer in use.

Disposal of external media/hardware/hardware

Disposal of external media

It must be assumed that any external media in the possession of an employee is likely to contain sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines

Requirements regarding equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Disposition of excess equipment

As the older Company computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.

- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

Change management

Statement of policy

To ensure that Company is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain Company sensitive information. Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated Company employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
    a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process if the change causes an adverse effect within the system and needs to be removed.

Audit controls

Statement of policy

To ensure that Company implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems. Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

Procedure

See policy entitled Information System Activity Review for the administrative safeguards for auditing system activities.

The Information Technology Services shall enable event auditing on all computers that process, transmit, and store for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of patient data being accessed for each attempted access. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.

The Company shall utilize appropriate network-based and host-based intrusion detection systems. The Information Technology Services shall be responsible for installing, maintaining, and updating such systems.

Information system activity review

Statement of policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Company shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Procedure

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Company's information systems.
2. The Information Technology Services shall be responsible for conducting reviews of Company's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.

4. Such reviews shall be conducted annually. Audits also shall be conducted if Company has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:
    a. **Logins.** Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
    b. **File accesses.** Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
    c. **Security incidents.** Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
    d. **User accounts.** Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format referred to in Section 2 of this policy and procedure.

5. The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Company's administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).

Contingency plan

Statement of policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems. Company is committed to

maintaining formal practices for responding to an emergency or other occurrence that damages systems. Company shall continually assess potential risks and vulnerabilities.

Procedure

1. Data Backup Plan
    a. Company shall implement a data backup plan to create and maintain retrievable exact copies
    b. At the end of each day, Monday through Friday, an incremental backup of all servers shall be backed up to tape. On Saturday, a full backup of all servers shall be backed up to tape. The backup tapes are taken each week off site by the IS Manager or his/her designee to ensure safeguard of Company's data. One month of backup data will always be maintained in a remote location. Backup media that is no longer in service will be disposed of in accordance with the Disposal of External Media/Hardware policy.
    c. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.
    d. The Security Officer shall test backup procedures on an annual basis to ensure that exact copies can be retrieved and made available. Such testing shall be documented by the Security Officer. To the extent such testing indicates need for improvement in backup procedures, the Security Officer shall identify and implement such improvements in a timely manner.
2. Disaster Recovery and Emergency Mode Operations Plan
    a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for:
    b. Restoring or recovering any loss of Company information and/or systems necessary to make systems available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
    c. Continuing operations during such time information systems are unavailable. Such written plan shall have enough level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan

shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

3. The disaster recovery and emergency mode operation plan shall include the following:
    a. Current copies of the information systems inventory and network configuration developed and updated as part of Company's risk analysis.
    b. Current copy of the written backup procedures developed and updated pursuant to this policy.
    c. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.
    d. Identification of an emergency response team. Members of such team shall be responsible for the following:
        i. Determining the impact of a disaster and/or system unavailability on Company's operations.
        ii. In the event of a disaster, securing the site and providing ongoing physical security.
        iii. Retrieving lost data.
        iv. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable
        v. Taking such steps necessary to restore operations.
    e. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of Company's risk analysis
    f. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:
        i. Members of the immediate response team
        ii. Facilities at which backup data is stored
        iii. Information systems vendors, and

iv. All current workforce members.

g. The disaster recovery team shall meet on at least an annual basis to:

i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Company

ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills

iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

Security awareness and training

Statement of policy

To establish a security awareness and training program for all members of Company's workforce, including management.

All workforce members shall receive appropriate training concerning Company's security policies and procedures. Such training shall be provided prior to the effective date and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

Procedure

1. Security Training Program

a. The Security Officer shall have responsibility for the development and delivery of initial security training. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.

b. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and

operational changes impacting the security of system addition of new hardware or software, and increased threats.

2. Security Reminders
    a. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.
    b. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.
3. Protection from Malicious Software
    a. As part of the Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
        i. Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
        ii. The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
        iii. Instructions to never download files from unknown or suspicious sources,
        iv. Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
        v. The importance of backing up critical data on a regular basis and storing the data in a safe place,
        vi. Damage caused by viruses and worms, and
        vii. What to do if a virus or worm is detected.

4. Password Management
    a. As part of the Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords
        i. Passwords must be changed every 90 days.
        ii. A user cannot reuse the last 12 passwords
        iii. Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.
        iv. Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
        v. A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.
        vi. Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to "fix" a computer or handle an emergency) or individuals, including family members.
        vii. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
        viii. Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
        ix. Any employee who is directed by the Security Officer to change his/her password to conform to the standards shall do so immediately.

Data breach response policy

Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards, and metrics (e.g., to enable prioritization of the

incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

The Company Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how ETA Transit, LLC 's established culture of openness, trust and integrity should respond to such activity. Company Information Security is committed to protecting ETA Transit, LLC 's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Company members. Any agreements with vendors will contain language similar that protects the fund.

Policy

Confirmed theft, data breach or exposure of Company Protected data or Company Sensitive data. As soon as a theft, data breach or exposure containing Company Protected data or Company Sensitive data is identified, the process of removing all access to that resource will begin. The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member services (if member data is affected)
- Human resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach, or exposure of Company data

The Executive Director will be notified of the theft, breach, or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with forensic investigators

As provided by Company cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with Company communications, legal and human resource departments to decide how to communicate the breach to a) internal employees, b) the public, and c) those directly affected.

Ownership and Responsibilities

Roles & Responsibilities:

- **Sponsors.** Sponsors are those members of the Company community that have primary responsibility for maintaining any information resource. Sponsors may be designated by any Company Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- **Information Security Administrator.** The Information Security Administrator is a member of the Company community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- **Users.** Users include virtually all members of the Company community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees, and volunteers.
- **Incident Response Team.** The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-

Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

Enforcement

Any Company personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

Appendix F: ETA price quote

This page was intentionally left blank.

Quotation #: 20230808-GoCOMO-AVLBAFO
Date: 9/14/2023

Agency: GoCOMO
Payment terms: See milestone payment schedule

etatransit.com

Received by: Date:

FIXED-ROUTE BASE SYSTEM

PRODUCT	ITEM#	QTY.	PRICE	TAX	TOTAL	MILE
Vehicle logic unit (VLU) hardware • GPS • Cellular communications • Vehicle I/O for 1708, DIO		25	$ 1,732	$ -	$ 43,300	1
Rugged mobile data terminal (MDT) hardware • 7" viewable screen ** 10" option available*		25	$ 309	$ -	$ 7,725	1
MDT mounting kit • RAM® mount		25	$ 252	$ -	$ 6,300	1
Master disconnect switch • to allow system to gracefully shut down		1	$ 53	$ -	$ 53	1
Bus equipment and cable kits • Power harness • Antennas • **Roof mount antennas available as an Option (extension cable required)*		25	$ 306	$ -	$ 7,650	1
Hardware installation • Professional system installation • Vehicle testing and commissioning		25	$ 600	$ -	$ 15,000	3

Single sign-on integrated with existing digital signage OPTIONAL • Integration of head signs with ITS ** Options for fare collection single sign-on* *** Options for MVS single sign-on*	0	$	250		$	-	3
Single sign-on integrated with existing fare collection OPTIONAL • Integration of digital fare collection system ** Options for fare collection single sign-on* *** Options for MVS single sign-on*	0	$	350		$	-	3
Implementation • System setup • Project management • Manufacturing • Training • Testing • Documentation • Travel	1	$	13,000		$	13,000	3
Software license: Public website • Real-time arrival predictions • Service messages • Rider feedback • Sponsored links • Station/stop details • Trip planner • Local attractions • Rider alerts • Favorite route selection	1	$	-		$	-	5
Software license: Native phone apps • Customized to local experience • Real-time bus tracking • Color-coded routes • Display user GPS location • Real-time arrival predictions • Trip planning • Rider feedback • Sponsored links • Local attractions • GTFS-RT rider alerts via push notifications	1	$	-		$	-	5

Software license: ETA SPOT™ API • JSON API • GTFS import/export	1	$	-		$ -	5
Annual SaaS and Maintenance: SPOT™ ITS • Unlimited user accounts • Data retention for the life of the contract • Real-time arrival predictions • Web-based dispatch module • Reports module • Route planner module • User administration module • Service announcements module • Cellular data • Hosting • Maintenance • 24/7/365 technical support • Daily backups (Qty. equals number of vehicles X 12 months)	300	$	75		$ 22,500	6

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$115,528
SALES TAX	INCLUDED
BASE SYSTEM TOTAL	**$115,528**
ANNUAL SaaS (BEYOND YEAR 1)	$22,500

AUTOMATIC VOICE ANNOUNCEMENTS (AVA)

Product	Item #	Qty.	Price	Tax	Total	Mile
Public address amplifier • Support automatic onboard announcements • Options for ambient noise sensing; automatic gain control ***ETA will attempt to reuse existing PA amplifiers if possible*** *Update 9/14/2023. With the understanding that PA amplifiers can be re-used, ETA has eliminated this charge*		0	$ 281	$ -	$ -	1

Public address amplifier installation • Professional system installation • Vehicle testing and commissioning *Update 9/14/2023. With the understanding that PA amplifiers can be re-used, ETA has eliminated this charge*	0	$	300	$	-	$ -	3
New monochromatic interior digital sign • Synchronize text with automatic onboard announcements audio	25	$	1,073	$	-	$ 26,813	1
Interior sign installation • Professional system installation • Vehicle testing and commissioning	25	$	300	$	-	$ 7,500	3
Implementation • System setup • Professional voice recordings * • Project management • Manufacturing • Training • Testing • Documentation • Travel ** recordings in additional languages shall be quoted separately as requested*	1	$	5,000			$ 5,000	3
Annual SaaS and Maintenance: SPOT™ AVA • Audio recording as a service • System support	300	$	5			$ 1,500	6

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$40,813
SALES TAX	INCLUDED
AVA TOTAL	**$40,813**
ANNUAL SaaS (BEYOND YEAR 1)	$1,500

AUTOMATIC PASSENGER COUNTING (APC) INTEGRATION

PRODUCT	ITEM#	QTY.	PRICE	TAX	TOTAL	MILE
Implementation (integration with TBD vendor) • System setup • Project management • Manufacturing • Training • Testing • Documentation • Travel *Update 9/14/2023: ETA reduces price from $25K to $0*		1	$ -		$ -	3
Annual SaaS and Maintenance: APC SaaS • Priced per bus, per month • Hosting • System maintenance and upgrades *Update 9/14/2023: ETA reduces price from $5 per bus/month to $0 per bus/month*		300	$ -		$ -	6

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$0
SALES TAX	INCLUDED
APC TOTAL	**$0**
ANNUAL SaaS (BEYOND YEAR 1)	$0

PACKAGE OPTIONS

Package	Qty.	Total
Fixed route base package	1	$ 115,528
Onboard announcements package	1	$ 40,813
Automatic passenger counting integration package	1	$ -
YEAR 1 PROJECT TOTAL		**$156,341**

ANNUAL CHARGES

Package	Qty.	Total
Fixed route base package annual subscription and maintenance	1	$22,500
Onboard announcements package annual subscription and maintenance	1	$1,500
Automatic passenger counting integration package annual subscription and maintenance	1	$0

ANNUAL CHARGES	$24,000
GRAND TOTAL 5 YEARS	**$252,341**

MILESTONE SCHEDULE

Mile	Description		Total	Deliverables
1	System design (50% Implementation costs)	$	20,250	Pre-installation site visit and documentation
2	Software licenses	$	-	Delivery of SPOT Console portal
3	Hardware components	$	91,841	Hardware delivery to customer location
4	Installation and vehicle static test (25% Implementation costs)	$	10,125	Hardware installation on first vehicle (by bus type) and static test report
5	Dynamic testing and training (25% implementation)	$	10,125	Dynamic test procedure report, training and manuals
6	Recurring items: Year 1	$	24,000	After 2 week burn-in (from customer-witnessed test) warranty; SaaS anniversary begins
7, 8, 9, 10	Recurring items: Years 2–5	$	96,000	Each SaaS anniversary

GRAND TOTAL 5 YEARS	**$252,341**

PREPARED BY:

NAME: John Maglio
TITLE: General Manager
ADDRESS: 7700 Congress Avenue, Suite 2201
Boca Raton, FL 33487
PHONE: (719) 453-0250
EMAIL: jpmaglio@etatransit.com

ADDITIONAL OPTIONS

PRODUCT	ITEM#	QTY.	PRICE	TAX	TOTAL	MILE
Extended warranty on hardware (Year 3) · Beyond year 2 (up to 5 years maximum) · Escalates at 3.5% per year · Does not include consumables · Governed by ETA's system support/warranty agreement · Provided as quoted, upon request	1	1	$ 4,592	$ -	$ 4,592	1
Extended warranty on hardware (Year 4) · Beyond year 2 (up to 5 years maximum) · Escalates at 3.5% per year · Does not include consumables · Governed by ETA's system support/warranty agreement · Provided as quoted, upon request	2	1	$ 4,753	$ -	$ 4,753	3
Extended warranty on hardware yr 5 · Beyond year 2 (up to 5 years maximum) · Escalates at 3.5% per year · Does not include consumables · Governed by ETA's system support/warranty agreement · Provided as quoted, upon request	3	1	$ 4,919	$ -	$ 4,919	3
Spare parts	4	1	$ 9,184	$ -	$ 9,184	5
Additional site visits (beginning beginning after acceptance) · On-site vehicle check up · Additional training *One analyst, 2 days* *Price per trip, as requested by customer*	5	0	$ 5,000	$ -	$ -	1
Data analyst services (after acceptance) · Senior data analyst to manager your route data · Routes, time tables, stop fences, system configuration, bus tracker customization *One analyst* *Price per year, as requested by customer*	6	0	$ 12,000	$ -	$ -	6

Time and material for change orders · Hourly labor rate · Applies to out of warrant repairs, custom software development, route manager changes...	7	0	$	200	$ -	$ -	6

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$23,448
SALES TAX	INCLUDED
TOTAL (YEAR 1)	**$23,448**
ANNUAL SaaS (BEYOND YEAR 1)	$0

Terms and conditions of sale

Unit prices are valid only for the total number of units quoted. Lesser quantities (or years) may require a higher price per unit cost because of certain fixed costs.

Prices in this quotation are valid for ninety (90) days from the date of quotation or proposal and are applicable to the quantities herein. Changes to packages and/or quantities may require a revised quotation.

No refund shall be provided for returned parts without written authorization from authorized ETA representatives.

Estimated lead time for delivery is 4 weeks. A formal lead time estimate shall be provided by ETA ARO.

Delivery is F.O.B. ETA Transit Systems, Inc. 7700 Congress Avenue #2201 Boca Raton, FL 33487

ETA TRANSIT SYSTEMS (ETA) WARRANTY POLICY

ETA guarantees that each product is free from defects in material and workmanship. ETA's warranty is in effect for two (2) years from the original ship date from ETA. ETA will furnish to customer its Warranty and Support agreement ARO or upon request

REVIEWED BY:

Nicole M Castonguay, CEO
ETA Transit Systems

Date:

ACCEPTED BY:

Signature: _____

Name and title: _____

Date: _____

GoCOMO – Exhibits and Pricing Page

[What you will discover]

Per the City of Columbia's RFP, this section are the required pricing page and exhibits.

[Section key points]

- GoCOMO Pricing Page
- Exhibit A – Offeror information
- Exhibit B – Current & prior experience
- Exhibit C – Expertise of personnel
- Exhibit D – Documentation of intent to participate
- Exhibit E – Method of performance
- Exhibit F – Work authorization affidavit
- Exhibit G – Miscellaneous information
- Exhibit H – Technical requirements

GoCOMO Pricing Page

This page was intentionally left blank.

4. PRICING PAGE

The offeror shall provide a firm, fixed price for an intelligent transportation system and services in accordance with the provisions and requirements stated herein as needed and requested through the term of the corresponding contract. The offeror shall provide an original contract period price and a maximum price for each potential renewal period.

Line Item	Description	Original Contract Period Firm, Fixed Price	1st Renewal Period Maximum Price	2nd Renewal Period Maximum Price	3rd Renewal Period Maximum Price	4th Renewal Period Maximum Price
1	Firm, Fixed Price for ITS Hardware (including installation)	**$3955 Per vehicle**	**$0 Per vehicle**	**$0 Per vehicle**	**$0 Per vehicle**	**$0 Per vehicle**
2	Firm, Fixed Price for ITS Software (including licenses)	**$2,992 Per vehicle**	**$0 Per vehicle**	**$0 Per vehicle**	**$0 Per vehicle**	**$0 Per vehicle**
3	Firm, Fixed Price for annual maintenance and support	**$1020 Per vehicle**	**$1020 Per vehicle**	**$1020 Per vehicle**	**$1020** Per vehicle	**$1020 Per vehicle**
4	Firm, Fixed Price for Training (including implementation)	**$0 Per hour**	**$0 Per hour**	**$0 Per hour**	**$0 Per hour**	**$0 Per hour**
5	Firm, Fixed Price for Cloud Storage	**$0 Per hour**	**$0 Per hour**	**$0 Per hour**	**$0 Per hour**	**$0 Per hour**
6	Firm, Fixed Price for Warranty (one time fee)	**$0** *2 year warranty included Ref. ETA's quote for extended warranty for years 3-5*				

Annual maximum percentage increase, above the previous contract term, after the initial five years of the contract:

5% increase per year after the initial 5 year term

_____%

Exhibit A – Offeror information

1. Provide a brief company history, including the founding date and number of years in business as currently constituted.
    a. Please reference “History” section Pg# 15 of the proposal.
2. Describe the nature of the vendor’s business, type of services performed, etc. Identify the vendor’s website address, if any.
    a. Please reference the “About Us” section Pg# 13 of the proposal.
    b. www.etatransit.com
3. Provide a list of and short summary of information regarding the vendor’s current contracts/clients.
    a. Please reference the “Customers” section Pg # 15 of the proposal
    b. The SPOT software is designed to support agencies of different scales and modes. including but not limited to rural, urban, and the university agencies.
        i. Over 50 active projects including: Toledo Area Regional Transit Authority, Valley Regional Transit, Space Coast Area Transit, City of Monroe - Transit, Lassen Rural Bus, City of Coral Gables, Danville Mass Transit, Clarksville Transit System, AppalCART, Stanford University, Auburn University, University of Southern California (USC)
4. List, identify and provide reasons for each contract/client gained and lost in the past two (2) years.
    a. New customers:
        i. Toledo Area Regional Transit Authority, AppalCART, USC, City of Davenport, City of Bettendorf, Hialeah Transit System, Hampton Roads Transit, City of Manteca, Auburn University, these contracts were awarded for a variety of reasons including: ultra reliable onboard equipment, high customer satisfaction scores/renewals, and a full featured software system.
    b. Lost:
        i. Tulsa Transit – A change of leadership, coupled with disparate views on long-term goals, culminated in a consensual decision to part ways.

Exhibit B – Current & prior experience

This section is not applicable to ETA Transit. There are no subcontractors for this project.

Exhibit C – Expertise of personnel

This page was intentionally left blank.

EXHIBIT C

EXPERTISE OF KEY PERSONNEL

(Copy and complete this table for each key person proposed**)**

Title of Position: Project Manager	
Name of Person:	Joshua Adler
Educational Degree (s): include college or university, major, and dates	Florida Atlantic University
License(s)/Certification(s), #(s), expiration date(s), if applicable:	Executive Certificate of Project Management - 2017
Specialized Training Completed.	Project Management -2017
# of years' experience in area of service proposed to provide:	6 Years
Describe person's relationship to offeror. If employee, # of years. If subcontractor, describe other/past working relationships	Employee - 4 years
Describe this person's responsibilities over the past 12 months.	Senior project manager for new implementations and upgrades
Previous employer(s), positions, and Dates	Duty Free Americas - Business Analayst/Project Manager 2011-2019

Staffing Methodology

Describe the person's planned duties/role proposed herein:	Project manager - Responsible for the implmentation for GoCOMO

List of Projects and Roles Completed

Describe the projects worked by the individual and the specific role:	Project manager - TARTA, USC, AppalCART, Davenport, Hialeah, and many more during his tenureship with ETA.

EXHIBIT C

EXPERTISE OF KEY PERSONNEL

(Copy and complete this table for each key person proposed**)**

Title of Position: Lead project engineer	
Name of Person:	James Warren
Educational Degree (s): include college or university, major, and dates	B.S. Electrical Engineering, University of Florida
License(s)/Certification(s), #(s), expiration date(s), if applicable:	
Specialized Training Completed.	
# of years' experience in area of service proposed to provide:	20 years of experience delivering complex transit technology solutions
Describe person's relationship to offeror. If employee, # of years. If subcontractor, describe other/past working relationships	Employee - 20 years with ETA Transit
Describe this person's responsibilities over the past 12 months.	Manager of support and field installations
Previous employer(s), positions, and Dates	

Staffing Methodology

Describe the person's planned duties/role proposed herein:	Manager for support and field installations

List of Projects and Roles Completed

Describe the projects worked by the individual and the specific role:	Tarta, Space Coast, Binghamton University, Auburn University and managing support tickets for all customers

EXHIBIT C

EXPERTISE OF KEY PERSONNEL

(Copy and complete this table for each key person proposed**)**

Title of Position: Customer experience advocate	
Name of Person:	Taylor Tanksley
Educational Degree (s): include college or university, major, and dates	Florida Atlantic University, B.S. Computer Science
License(s)/Certification(s), #(s), expiration date(s), if applicable:	
Specialized Training Completed.	
# of years' experience in area of service proposed to provide:	3 years
Describe person's relationship to offeror. If employee, # of years. If subcontractor, describe other/past working relationships	Employee - 3 years
Describe this person's responsibilities over the past 12 months.	Customer advocate for new implementations and responding to support tickets as assigned
Previous employer(s), positions, and Dates	

Staffing Methodology

Describe the person's planned duties/role proposed herein:	Customer advocate and dedicated support representative

List of Projects and Roles Completed

Describe the projects worked by the individual and the specific role:	Space Coast Transit, Auburn, DFW, Coral Gables

Exhibit D – Documentation of intent to participate

This section is not applicable to ETA Transit. There are no subcontractors for this project.

Exhibit E – Method of performance

1. Offeror must explain how long data is kept in the system.
    a. Key data is stored for the life of the contract.
2. Offeror must detail how data is secured from unauthorized access.
    a. Reference “Appendix E”, Pg # 150 of the proposal
3. Offeror must explain warranty information for all components, including hardware and software.
    a. Reference “Warranty overview” section Pg # 125 of the proposal

Exhibit F – Work authorization affidavit

This page was intentionally left blank.

EXHIBIT F

NOTICE TO OFFERORS

Sections 285.525 To 285.550 RSMo.

Pursuant to section 285.530 (1) RSMo., No business entity or employer shall knowingly employ, hire for employment, or continue to employ an unauthorized alien to perform work within the State of Missouri.

As a condition for the award of any contract or grant in excess of five thousand dollars by the state or by any political subdivision of the state to a business entity, or for any business entity receiving a state-administered or subsidized tax credit, tax abatement, or loan from the state, the business entity shall, by sworn affidavit and provision of documentation, affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services. Every such business entity shall sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. {RSMo 285.530 (2)}

An Employer may enroll and participate in a federal work authorization program and shall verify the employment eligibility of every employee in the employer's hire whose employment commences after the employer enrolls in a federal work authorization program. **The E-verify system issues a Memorandum of Understanding once enrollment is complete; the City of Columbia requires a copy of this document be attached to the Work Authorization Affidavit.** The employer shall retain a copy of the dated verification report received from the federal government. Any business entity that participates in such program shall have an affirmative defense that such business entity has not violated subsection 1 of this section. {RSMo 285.530 (4)}

For offerors that are not already enrolled and participating in a federal work authorization program, E-Verify is an example of this type of program. Information regarding E-Verify is available at:
http://www.dhs.gov/e-verify

EXHIBIT F, Continued
CITY OF COLUMBIA, MISSOURI
WORK AUTHORIZATION AFFIDAVIT
PURSUANT TO 285.530 RSMo
(FOR ALL BIDS IN EXCESS OF $5,000.00)

County of Palm Beach)
)SS.
State of Florida)

My name is Nicole Castonguay. I am an authorized agent of ETA Transit Systems (Bidder). This business is enrolled and participates in a federal work authorization program for all employees working in connection with services provided to the City of Columbia. This business does not knowingly employ any person who is an unauthorized alien in connection with the services being provided. **Documentation of participation in a federal work authorization program is attached to this affidavit.**

Furthermore, all subcontractors working on this contract shall affirmatively state in writing in their contacts that they are not in violation of Section 285.530.1 RSMo and shall not thereafter be in violation. Alternatively, a subcontractor may submit a sworn affidavit under penalty of perjury that all employees are lawfully present in the United States.

Nicole Castonguay
Affiant

Nicole Castonguay
Printed Name

Personally appeared before me, a Notary Public, within and for the County of Palm Beach,

State of Missouri, the person whose signature appears above, PERSONALLY AND KNOWN TO ME AND ACKNOWLEDGED, that signed the foregoing Affidavit for the purposes therein stated.

Subscribed and sworn to me this 18 day of July, 2023.

My Commission expires April 2, 2027.

Bessy Prager
(Notary Public)

BESSY PRAGER
Notary Public - State of Florida
Commission # HH 381875
My Comm. Expires Apr 2, 2027
Bonded through National Notary Assn.

Exhibit G – Miscellaneous information

This page was intentionally left blank.

EXHIBIT G

MISCELLANEOUS INFORMATION

Employee/Conflict of Interest:

Offerors who are elected or appointed officials or employees of the City of Columbia or any political subdivision thereof, serving in an executive or administrative capacity, must comply with sections 105.450 to 105.458, RSMo, regarding conflict of interest. If the offeror or any owner of the offeror's organization is currently an elected or appointed official or an employee of the City of Columbia or any political subdivision thereof, please provide the following information:	
Name and title of elected or appointed official or employee of the City of Columbia or any political subdivision thereof:	Not applicable
If employee of the City of Columbia or political subdivision thereof, provide name of City or political subdivision where employed:	Not applicable
Percentage of ownership interest in offeror's organization held by elected or appointed official or employee of the City of Columbia or political subdivision thereof:	0 _____%

Registration of Business Name (if applicable) with the Missouri Secretary of State

The offeror should indicate the offeror's charter number and company name with the Missouri Secretary of State. Additionally, the offeror should provide proof of the offeror's good standing status with the Missouri Secretary of State. If the offeror is exempt from registering with the Missouri Secretary of State pursuant to section 351.572, RSMo., identify the specific section of 351.572 RSMo., which supports the exemption.

	ETA Phi Systems, Inc
Charter Number (if applicable)	***Company Name***
If exempt from registering with the Missouri Secretary of State pursuant to section 351.572 RSMo., identify the section of 351.572 to support the exemption: Upon being awarded the contract, ETA Transit will proceed to complete the necessary registration with the State of Missouri	

Exhibit H – Technical requirements

This page was intentionally left blank.

EXHIBIT H

TECHNICAL REQUIREMENTS

Key*	Description
F	**Fully functional**, provided "Commercial Off-The-Shelf (COTS)"
CU	**Customization** (Change to source code required)
CO	**Configuration** (Setup required with built-in tools and procedures but no change to source code is required.)
TP	**Third-Party** (Additional software required to provide Requirement.)
R	Provided with **Reporting** Tool
NA	**Not Available**

The Vendor must complete this checklist by indicating at what level each requirement can be met. Please respond by entering the appropriate **Key** code next to each requirement. Vendors should also use the comments section to further explain how their proposed solution meets the requirement.

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.1 General Application Requirements				
A.1.1	**M**	The cloud vendor shall adhere to WCAG 2.1 Level AA compliance for web hosted solutions and/or SaaS offerings that are web based in accordance with the Americans with Disabilities Act and its implementing regulations and guidance.	F	
A.1.2	**M**	The City shall be entitled to any and all **upgraded versions** of the solution covered in the contract.	F	
A.1.3	**M**	The Vendor shall provide **free and timely upgrades** to the software when published.	F	
A.1.4	**O**	If applicable, software fixes and enhancements for other client implementations shall be made available to the City at no charge.	F	
A.1.5	**M**	All patches, upgrades and updates shall be **coordinated** with the City to ensure proper planning and notifications.	F	
A.1.6	**M**	The solution shall provide well-defined **change management** processes, including pre-defined all-inclusive migration processes for software releases, operating system upgrades, layered software upgrades, and hardware configuration changes.	F	
A.1.7	**O**	The solution shall support Electronic Data Interchange (EDI).	F	
A.1.8	**M**	The solution shall comply with all current applicable **government standards** and web-based transaction encryption standards identified by the City (i.e. HIPAA, CJIS, NERC/CIP, PCI, etc.)	NA	
A.1.9	**O**	The solution shall provide customizable user interfaces.	F	

A.1.10	**M**	The software vendor shall provide client support and maintenance with **Service Level Agreements** based on case severities.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.1 General Application Requirements (continued)				
A.1.12	**O**	Application source code shall be placed in **escrow**.	NA	
A.1.13	**M**	The solution shall provide the ability to maintain and update **non-production environment**(s).	F	
A.1.13	**M**	The solution shall provide the ability to apply software upgrades to non-production environment(s) before applying to a production environment.	F	
A.1.14	**M**	The solution shall have the capability to present users with **tools which are relevant** in the current context, eliminating or disabling irrelevant tools. It should use progressive disclosure to reveal information as it is needed and give users the option to hide information they don't consider useful.	F	
A.1.15	**O**	The solution functionality shall provide intelligent support related to **drop-down table entries**. For example, it should be possible to select items in a list by clicking on the desired choice or typing as much of the item description as is needed to uniquely identify it (similar to the Microsoft Outlook address book). It should be possible to type an exact value into a table-validated field.	F	
A.1.16	**M**	The solution shall **ensure key data persists** as the user moves from one window (screen) to the next, to minimize re-entry and mistakes.	F	
A.1.17	**O**	The solution shall provide means to **validate data** by checking entered values against a list of valid values maintained in tables by City or service provider personnel.	F	
A.1.18	**O**	The solution shall allow both interactive and batch entry of data.	F	
A.1.19	**O**	The solution shall accommodate background **(batch) jobs** concurrently without interrupting normal business operations.	F	
A.1.20	**M**	The solution shall **validate all transactions** for errors and provide immediate user feedback, including error messages and possible corrective actions.	F	
A.1.21	**O**	The solution shall provide support for **inter-process communication** including, but not limited to, the following: • *Attachment of standard object types in an object library* • *Cut and paste capability from data fields and screens to other applications.*	F	
A.1.22	**M**	The solution shall be **compliant** with open standards such as but not limited to SMTP, SNMP, and SFTP.	F	
A.1.23	**O**	The solution shall contain an **API** to assist with integrations.	F	

A.1.24	**M**	Software shall run with **least possible privilege**. It should not run as a user that has access outside of its need.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.2 General Database and Reporting Requirements				
A.2.1	**M**	Solution shall support **SQL Server 2017** Standard or above.	F	
A.2.2	**M**	The solution shall allow **insertion of data** from a third party tool, i.e. Digital Transformation Services (DTS) or SQL Server Integration Services (SSIS), for at least basic setup of tables or synchronization points, i.e. vendor lists, contacts, etc.	NA	SAAS Solution
A.2.3	**O**	Additional ad-hoc reporting capabilities shall be available utilizing **Crystal Reports or SSRS** (SQL Server Reporting Services).	NA	SAAS Solution
A.2.4	**M**	The solution shall use and maintain a ***primary key*** across all Databases / Tables.	NA	SAAS Solution
A.2.5	**M**	The solution shall utilize appropriate database rules and constraints to enforce and maintain **referential integrity**.	NA	SAAS Solution
A.2.6	**M**	The solution shall provide for **simultaneous** access to data by concurrent users.	NA	SAAS Solution
A.2.7	**M**	The solution shall provide standard structured query language (**SQL**) capabilities for database queries.	NA	
A.2.8	**O**	The solution shall provide the ability to **lock** database records at a row and column level.	NA	
A.2.9	**O**	The solution shall allow for **data replication** for disaster recovery.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.3 General Infrastructure Requirements				
A.3.1	**M**	The solution shall operate on a platform which provides **extensibility, redundancy, scalability, reliability and connectivity**.	F	
A.3.2	**M**	The solution shall use **TCP/IP** and subsequent standards as approved by IEEE as the standard network protocol.	F	
A.3.3	**O**	The solution shall integrate with the City's **Active Directory (Federated) Services / LDAP** for Single sign-on.	F	
A.3.4	**O**	The solution shall provide email integrations via **SMTP/S.**	F	
A.3.5	**O**	The solution shall support dynamic **load balancing** and automatic fail-over between multiple servers.	F	
A.3.6	**M**	The solution shall maintain data integrity to **mitigate data loss** and/or corruption.	F	
A.3.7	**M**	The solution shall accommodate **unattended backup** of critical system tables, transaction logs, files, operating system and other information by allowing full, incremental and live backups.	F	
A.3.8	**M**	The solution shall be able to accommodate recovery practices (**restore from backup**) in the event of a qualifying data event.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.4 General Workstation / Hardware Compatibility Requirements				
A.4.1	**M**	The solution shall support, at a minimum, 32-bit IBM-compatible, 16 GB RAM, 250 GB hard drive personal computer (desktop or laptop) with **Microsoft Windows 10** operating system.	F	
A.4.2	**M**	The solution shall be compatible with **Trend Micro Apex One 2019** anti-virus software.	F	
A.4.3	**M**	If accessed from a browser, the solution shall be compatible with **Chrome**, FireFox, or Microsoft Edge. Vendor must provide list of compatible versions and any other items related to browser-based solutions.	F	
A.4.4	**M**	The City utilizes Google Workspace Apps and **Gmail**. The solution shall be able to interface with these technologies.	F	
A.4.5	**O**	If scanners are required, the solution shall be compatible with TWAIN **scanners.** The city currently utilizes the following: - Canon DR-2580C, DR-M140 - EPSON DS-510, ES-400	NA	
A.4.6	**O**	If printing is required, the solution shall be compatible with the following **printers**: - CANON / Image Runner C5235 - CANON / iR-ADV C9280-A2 - HP Color LaserJet M750 - HP Color LaserJet MFP 400, M476dn, M570DN, M680 - HP LaserJet M630, M652dn - HP LaserJet MFP M4345, M4555, M830z - Sharp MX-3071, MX-4071, MX-4072, MX-B476W, MX-M3071, MX-M3571, MX-M4071	NA	
A.4.7	**M**	The software shall run as standard user (without administrative privileges)	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.5 General Security Requirements				
A.5.1	**O**	The solution shall provide the capability to support **public/private key encryption**.	F	
A.5.2	**M**	Vendor shall **encrypt** City data while in storage (at rest), in transit, on backup media, and provide decryption means.	NA	SAAS Solution
A.5.3	**M**	The solution shall provide an **audit trail** for tracking changes for what was changed, who made the change, and when the change was made. Including but not limited to the following: • *Applications* • *User Access* • *Database Modifications*	F	
A.5.4	**M**	The solution shall disable a user account if a defined number of **unsuccessful login attempts** are made within a defined time period.	F	
A.5.5	**M**	The solution shall automatically log users off of the application running on a workstation after a defined period of **inactivity** on that workstation.	F	
A.5.6	**M**	The solution shall provide **security control**, audit and setup capabilities for the system administrator.	F	
A.5.7	**M**	The system administrator shall be able to establish new users, remove users, update users, lock users and to set **security access** rights for users that both restrict and allow access to solution capabilities.	F	
A.5.8	**O**	The solution shall support multi-factor authentication.	CU	
A.5.9	**M**	The solution shall not transmit, display or store User ID's or passwords in **clear text**.	F	
A.5.10	**M**	System account names shall be unique. Passwords should meet minimum complexity standards as defined by the City. Length: 15; Requires 1 lower case, 1 upper case, 1 number and 1 special character.	CO	
A.5.11	**M**	**The solution shall never use default user names and passwords, including hard-coded accounts.**	F	
A.5.12	**M**	The vendor shall not deploy services to the City of Columbia where system accounts are shared with other entities.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.6 Cloud Hosted / SaaS Requirements (complete if applicable)				
A.6.1	**M**	The solution **high availability** standard shall be greater than or equal to 99.99%.	F	
A.6.2	**M**	The solution shall include at minimum, a **256 bit** encrypted SSL Certificate from a Certificate Authority (not self-signed).	F	
A.6.3	**M**	**All data must remain in the Continental United States** of America, including replication, backups and off-site storage.	F	
A.6.4	**M**	The solution must be **hosted** within the Continental United States of America.	F	
A.6.5	**M**	All City data stored in the cloud is the **property of the City**. Data shall remain accessible, queryable and exportable during the duration of the agreement.	F	
A.6.6	**M**	Vendor shall work with City to provide all data in an acceptable format upon termination of the agreement. Data housed by vendor or its hosting provider shall be destroyed within 30 days and a certificate of destruction provided as verification.	F	
A.6.7	**M**	Vendor shall respond to **records requests** within the timeframe stated in the agreement. The vendor shall accept liability if the records request is not fulfilled in the agreed upon timeframe.	F	
A.6.8	**O**	All cloud deployments that are intended to perform a service for our customers shall be deployed using City of Columbia owned **domain names**. The vendor shall not expect to maintain DNS records belonging to the City.	F	
A.6.9	**O**	Vendor shall provide the **IP addresses** used for City of Columbia domain name service prior to deployment. The vendor shall not change the IP addresses used with a frequency of greater than once per year. The vendor shall notify the City IT department in writing on official letterhead 30 days in advance of any IP address changes.	NA	SAAS Solution
A.6.10	**O**	Vendor shall conform to the City's DKIM and DMARC requirements for email. SPF record needs to be limited to certain IP's or be sent from a como.gov subdomain.	NA	SAAS Solution
A.6.11	**M**	Vendor shall take all reasonable precautions to ensure that **SPAM** is not sent using the CoMo.gov domain or from any IP address under vendor control that has been associated with the CoMo.gov domain.	NA	SAAS Solution
A.6.12	**M**	Vendor shall react to **email abuse** reports in a timely manner.	NA	SAAS Solution
A.6.13	**M**	Vendor shall conduct **regular security audits** of their solution. The security audits shall include internal and external review of solution security and the security of all code used by the vendor. The vendor shall react promptly to mitigate the vulnerabilities identified by security audits.	F	
A.6.14	**M**	Vendor shall apply all **system patches** within 30 days of release. Critical system patches shall be applied immediately after testing.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.6 Cloud Hosted / SaaS Requirements (continued)				
A.6.15	**M**	Vendor shall have a 24x7x365 method for reporting and correcting discovered **vulnerabilities**. Vulnerabilities should be prioritized and corrected based on the risk vulnerability exploitation would pose to its customers. Vulnerability mitigation efforts should be tested by the vendor, as appropriate, prior to their release.	F	
A.6.16	**M**	Vendor shall take responsibility for **security incident handling** if their solution is compromised.	F	
A.6.17	**M**	Vendor shall immediately notify the City of any **breaches** and will advise what information has been compromised. If this information is later found to be inaccurate the cloud vendor will immediately notify the City with the correct information.	F	
A.6.18	**M**	If investigation, containment, and eradication efforts by the City incur costs while fault lies with the vendor, the vendor shall assume the costs.		
A.6.19	**M**	Vendor shall provide their **incident response plans**. Response plans will include procedures for both security and disaster incident response.	F	

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.7 On-Premises (Hosted by City) Requirements (complete if applicable)				
A.7.1	**M**	All data for the solution shall be **directly accessible** with major industry standard data access tools for use in reporting and integration with other City systems.	NA	SAAS Solution
A.7.2	**M**	Production and non-production databases shall remain **separate** and not reside on the same database server.	NA	SAAS Solution
A.7.3	**M**	The solution shall be Open Database Connectivity (**ODBC**) compliant.	NA	SAAS Solution
A.7.4	**O**	The solution shall provide documented **best practices** including but not limited to optimum database and client maintenance.	NA	SAAS Solution
A.7.5	**M**	The solution shall be able to run on a minimum of **VMWare ESXi 7** virtual infrastructure.	NA	SAAS Solution
A.7.6	**M**	The solution shall be able to run on **Windows Server 2019** Standard or above.	NA	SAAS Solution
A.7.7	**M**	The solution shall support, at a minimum, **64-bit** back-end (server) processing including but not limited to multiprocessors and multi-threaded processes.	NA	SAAS Solution
A.7.8	**M**	The solution shall be compatible with Trend Micro Apex One 2019 **anti-virus software**. Please list exceptions or concerns in comments.	NA	SAAS Solution
A.7.10	**M**	The solution shall permit **operating system patching and updates**, and allow for a system restart when a patch or update requires it.	NA	SAAS Solution
A.7.11	**M**	**Remote vendor access** for support shall be accomplished through secured methods.	NA	SAAS Solution

Req. No.	Mandatory/ Optional Requirement	Requirement	Key*	Comments
A.8 Implementation, Training and Support Requirements				
A.8.1	**M**	Vendor shall include in the **Implementation Plan** the ways and means of how the implementation shall be managed, including, but not limited to schedule, risk, and quality.	F	
A.8.2	**M**	Vendor shall include in the Implementation Plan the descriptions of the **vendor roles** and responsibilities during the solution implementation.	F	
A.8.3	**M**	Vendor shall include in the Implementation Plan the descriptions of the **City's roles** and responsibilities during the solution implementation.	F	
A.8.4	**M**	Vendor shall state in the Implementation Plan **assumptions and expectations** for both the vendor and City stakeholders, in order to reduce any and all ambiguity during the implementation.	F	
A.8.5	**O**	Vendor shall include in the Implementation Plan the process for **loading data** into reference tables, such as users, roles, etc.	F	
A.8.6	**O**	Vendor shall include in the implementation plan any **conversion** services required.	F	
A.8.8	**M**	Vendor shall provide application **support** by phone (toll-free) and email during normal business hours (8:00 A.M. - 5:00 P.M.CST, M-F).	F	
A.8.9	**M**	Vendor **training** should not be done on production systems/data.	F	
A.8.10	**O**	Vendor shall provide a comprehensive description of the ***technical* training** available to the City for the solution.	F	
A.8.11	**M**	Vendor shall provide a comprehensive description of the ***functional* training** available to the City for the solution.	F	

Dear Evaluation Committee of Go Como,

We extend our gratitude for affording us the opportunity to submit our Best and Final Offer (BAFO) pricing in response to RFP 128/2023 concerning Intelligent Transportation Systems Services.

We are pleased to confirm that ETA's proposal fulfills the essential criteria outlined in the RFP, comprehensively illustrating how we intend to meet the specified requirements. Moreover, we have taken the initiative to enhance the attractiveness of our proposal by reducing the cost component.

We are delighted to inform you that ETA has adjusted its pricing from an initial figure of $299,366 down to $252,341, representing a notable cost reduction of approximately 16%.

For your convenience, we have included two vital documents with this communication:

Document titled "128.2023 BAFO 1 Pricing Page - ETA Transit.pdf" - This contains the updated pricing form as per the City's requirements.

Document titled "GoCOMO AVL RFP BAFO_9.14.2023" - This provides ETA's detailed quotation in our specific format. Notably, it employs red font to highlight precisely where the cost savings have been achieved.

Thank you for considering our revised proposal. We remain at your disposal for any further inquiries or discussions.

Sincerely,

John P Maglio
President
[C] (561) 314-5660

Line	Description	Cost	
1	Firm Fixed Price for Year One including ITS Hardware (including installation), Software (Including licenses), maintenance and support, training for an estimated 14 individuals, cloud storage and warranty for 25 Vehicles.	$	156,341
2	Firm Fixed Price for maintenance and support, and software for year 2	$	24,000
3	Firm Fixed Price for maintenance and support, and software for year 3	$	24,000
4	Firm Fixed Price for maintenance and support, and software for year 4	$	24,000
5	Firm Fixed Price for maintenance and support, and software for year 5	$	24,000
6	List any additional costs that are not included above. These will be evaluated subjectively in the method of performance scoring criteria section.	$	-

Quotation #: 20230808-GoCOMO-AVLBAFO
Date: 9/14/2023

Agency: GoCOMO
Payment terms: See milestone payment schedule

etatransit.com | Received by: | Date:

FIXED-ROUTE BASE SYSTEM

PRODUCT	ITEM#	QTY.	PRICE	TAX	TOTAL	MILE	CAT
Vehicle logic unit (VLU) hardware • GPS • Cellular communications • Vehicle I/O for 1708, DIO		25	$ 1,732	$ -	$ 43,300	1	1
Rugged mobile data terminal (MDT) hardware • 7" viewable screen ** 10" option available*		25	$ 309	$ -	$ 7,725	1	1
MDT mounting kit • RAM® mount		25	$ 252	$ -	$ 6,300	1	1
Master disconnect switch • to allow system to gracefully shut down		1	$ 53	$ -	$ 53	1	1
Bus equipment and cable kits • Power harness • Antennas • **Roof mount antennas available as an Option (extension cable required)*		25	$ 306	$ -	$ 7,650	1	1
Hardware installation • Professional system installation • Vehicle testing and commissioning		25	$ 600	$ -	$ 15,000	3	1
Single sign-on integrated with existing digital signage OPTIONAL • Integration of head signs with ITS ** Options for fare collection single sign-on* *** Options for MVS single sign-on*		0	$ 250		$ -	3	1

Single sign-on integrated with existing fare collection OPTIONAL • Integration of digital fare collection system ** Options for fare collection single sign-on* *** Options for MVS single sign-on*	0	$	350		$	-	3	1
Implementation • System setup • Project management • Manufacturing • Training • Testing • Documentation • Travel	1	$	13,000		$	13,000	3	2
Software license: Public website • Real-time arrival predictions • Service messages • Rider feedback • Sponsored links • Station/stop details • Trip planner • Local attractions • Rider alerts • Favorite route selection	1	$	-		$	-	5	2
Software license: Native phone apps • Customized to local experience • Real-time bus tracking • Color-coded routes • Display user GPS location • Real-time arrival predictions • Trip planning • Rider feedback • Sponsored links • Local attractions • GTFS-RT rider alerts via push notifications	1	$	-		$	-	5	2
Software license: ETA SPOT™ API • JSON API • GTFS import/export	1	$	-		$	-	5	2

Annual SaaS and Maintenance: SPOT™ ITS • Unlimited user accounts • Data retention for the life of the contract • Real-time arrival predictions • Web-based dispatch module • Reports module • Route planner module • User administration module • Service announcements module • Cellular data • Hosting • Maintenance • 24/7/365 technical support • Daily backups (Qty. equals number of vehicles X 12 months)	300	$	75		$	22,500	6	3

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$115,528
SALES TAX	INCLUDED
BASE SYSTEM TOTAL	**$115,528**
ANNUAL SaaS (BEYOND YEAR 1)	$22,500

AUTOMATIC VOICE ANNOUNCEMENTS (AVA)

Product	Item #	Qty.		Price	Tax		Total		Mile	
Public address amplifier • Support automatic onboard announcements • Options for ambient noise sensing; automatic gain control *ETA will attempt to reuse existing PA amplifiers if possible* *Update 9/14/2023. With the understanding that PA amplifiers can be re-used, ETA has eliminated this charge*		0	$	281	$	-	$	-	1	1

Public address amplifier installation • Professional system installation • Vehicle testing and commissioning *Update 9/14/2023. With the understanding that PA amplifiers can be re-used, ETA has eliminated this charge*	0	$	300	$ -	$	-	3	1
New monochromatic interior digital sign • Synchronize text with automatic onboard announcements audio	25	$	1,073	$ -	$	26,813	1	1
Interior sign installation • Professional system installation • Vehicle testing and commissioning	25	$	300	$ -	$	7,500	3	1
Implementation • System setup • Professional voice recordings * • Project management • Manufacturing • Training • Testing • Documentation • Travel ** recordings in additional languages shall be quoted separately as requested*	1	$	5,000		$	5,000	3	2
Annual SaaS and Maintenance: SPOT™ AVA • Audio recording as a service • System support	300	$	5		$	1,500	6	3

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$40,813
SALES TAX	INCLUDED
AVA TOTAL	**$40,813**
ANNUAL SaaS (BEYOND YEAR 1)	$1,500

AUTOMATIC PASSENGER COUNTING (APC) INTEGRATION

PRODUCT	ITEM#	QTY.	PRICE	TAX	TOTAL	MILE

Implementation (integration with TBD vendor) • System setup • Project management • Manufacturing • Training • Testing • Documentation • Travel *Update 9/14/2023: ETA reduces price from $25K to $0*	1	$	-		$	-	3	2
Annual SaaS and Maintenance: APC SaaS • Priced per bus, per month • Hosting • System maintenance and upgrades *Update 9/14/2023: ETA reduces price from $5 per bus/month to $0 per bus/month*	300	$	-		$	-	6	3

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$0
SALES TAX	INCLUDED
APC TOTAL	**$0**
ANNUAL SaaS (BEYOND YEAR 1)	$0

PACKAGE OPTIONS

Package	Qty.		Total
Fixed route base package	1	$	115,528
Onboard announcements package	1	$	40,813
Automatic passenger counting integration package	1	$	-
YEAR 1 PROJECT TOTAL			**$156,341**

ANNUAL CHARGES

Package	Qty.	Total
Fixed route base package annual subscription and maintenance	1	$22,500
Onboard announcements package annual subscription and maintenance	1	$1,500

Automatic passenger counting integration package annual subscription and maintenance	1	$0

ANNUAL CHARGES	$24,000
GRAND TOTAL 5 YEARS	**$252,341**

PREPARED BY:

NAME: John Maglio
TITLE: General Manager
ADDRESS: 7700 Congress Avenue, Suite 2201
Boca Raton, FL 33487
PHONE: (719) 453-0250
EMAIL: jpmaglio@etatransit.com

ADDITIONAL OPTIONS

PRODUCT	ITEM#	QTY.	PRICE	TAX	TOTAL	MILE
Extended warranty on hardware (Year 3) · Beyond year 2 (up to 5 years maximum) · Escalates at 3.5% per year · Does not include consumables · Governed by ETA's system support/warranty agreement · Provided as quoted, upon request	1	1	$ 4,592	$ -	$ 4,592	1
Extended warranty on hardware (Year 4) · Beyond year 2 (up to 5 years maximum) · Escalates at 3.5% per year · Does not include consumables · Governed by ETA's system support/warranty agreement · Provided as quoted, upon request	2	1	$ 4,753	$ -	$ 4,753	3
Extended warranty on hardware yr 5 · Beyond year 2 (up to 5 years maximum) · Escalates at 3.5% per year · Does not include consumables · Governed by ETA's system support/warranty agreement · Provided as quoted, upon request	3	1	$ 4,919	$ -	$ 4,919	3
Spare parts	4	1	$ 9,184	$ -	$ 9,184	5

Additional site visits (beginning beginning after acceptance) · On-site vehicle check up · Additional training *One analyst, 2 days* *Price per trip, as requested by customer*	5	0	$	5,000	$	-	$	-	1
Data analyst services (after acceptance) · Senior data analyst to manager your route data · Routes, time tables, stop fences, system configuration, bus tracker customization *One analyst* *Price per year, as requested by customer*	6	0	$	12,000	$	-	$	-	6
Time and material for change orders · Hourly labor rate · Applies to out of warrant repairs, custom software development, route manager changes...	7	0	$	200	$	-	$	-	6

Tax exempt certificate required for sales tax to be waived.

SUBTOTAL	$23,448
SALES TAX	INCLUDED
TOTAL (YEAR 1)	**$23,448**
ANNUAL SaaS (BEYOND YEAR 1)	$0

Terms and conditions of sale

Unit prices are valid only for the total number of units quoted. Lesser quantities (or years) may require a higher price per unit cost because of certain fixed costs.

Prices in this quotation are valid for ninety (90) days from the date of quotation or proposal and are applicable to the quantities herein. Changes to packages and/or quantities may require a revised quotation.

No refund shall be provided for returned parts without written authorization from authorized ETA representatives.

Estimated lead time for delivery is 4 weeks. A formal lead time estimate shall be provided by ETA ARO.

Delivery is F.O.B. ETA Transit Systems, Inc. 7700 Congress Avenue #2201 Boca Raton, FL 33487

ETA TRANSIT SYSTEMS (ETA) WARRANTY POLICY

ETA guarantees that each product is free from defects in material and workmanship. ETA's warranty is in effect for two (2) years from the original ship date from ETA. ETA will furnish to customer its Warranty and Support agreement ARO or upon request

REVIEWED BY:

Nicole M Castonguay, CEO Date:
ETA Transit Systems

ACCEPTED BY:

Signature: _____

Name and title: _____

Date: _____