

Contract # MA3696

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Division of Purchasing and the following Contractor:

USCC Services, LLC

Name

UScellular Department 205

Address

Palatine

IL

60055-0205

City

State

Zip

LEGAL STATUS OF CONTRACTOR

- ☐ Sole Proprietor
☐ Non-Profit Corporation
☒ For-Profit Corporation
☐ Partnership
☐ Government Agency

Contact Person Kathryn Swick Phone #331-645-4818 Email Kathryn.swick@uscellular.comVendor # VC247908 Commodity Code # 43190

2. CONTRACT PORTFOLIO NAME: Wireless Voice, Data and Accessories
3. GENERAL PURPOSE OF CONTRACT: The general purpose of this contract is to provide: IOT Award
4. PROCUREMENT: This contract is entered into as a result of the procurement process on Bid# CJ21-3.
5. CONTRACT PERIOD: Effective Date: 5/20/2021 Termination Date: 8/11/2024 unless terminated early or extended in accordance with the terms and conditions of this contract. Renewal options (if any): One Five (5) year extension option.
6. Payment: Prompt Payment Discount (if any): N/A.
7. Administrative Fee, as described in the Solicitation and Attachment A.
8. ATTACHMENT A: Master Terms and Conditions
 ATTACHMENT B: Scope of Work
 ATTACHMENT C: Cost Sheet
 ATTACHMENT G: Plan Description
 ATTACHMENT R: Financial Attestation
 ATTACHMENT S: Security Disclosure
 ATTACHMENT T: Technical Questionnaire
 ATTACHMENT V: Subcategory Definitions
 ATTACHMENT W: Contractor Award Sheet
Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.
9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
 - Utah State Procurement Code, Procurement Rules, and Contractor's response to solicitation #CJ21-3.
10. Each person signing this Agreement represents and warrants that he/she is duly authorized and has legal capacity to execute and deliver this Agreement and bind the parties hereto. Each signatory represents and warrants to the other that the execution and delivery of the Agreement and the performance of each party's obligations hereunder have been duly authorized and that the Agreement is a valid and legal agreement binding on the parties and enforceable in accordance with its terms.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR
 DocuSigned by:

STATE

5/26/2021 | 3:19 PM CDT

06/09/2021

Contractor's signature

Date

Director, Division of Purchasing

Date

Katie Swick Director of Business Sales Operations & Enablement

Type or Print Name and Title

Christopher Jennings

Division of Purchasing Contact Person

801-957-7151

Telephone Number

N/A

Fax Number

ctjennings@utah.gov

Email



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

- (1) A Participating Entity's Participating Addendum ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions;
- (3) A Purchase Order issued against the Master Agreement;
- (4) The Specifications or Statement of Work;
- (5) The Solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions;
- (6) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions

Acceptance is defined by the applicable commercial code, except Acceptance shall not occur before the completion of delivery in accordance with the Order, installation if required, and a reasonable time for inspection of the Product.

Contractor means the person or entity delivering Products or performing services under the terms and conditions set forth in this Master Agreement.

Embedded Software means one or more software applications which permanently reside on a computing device.

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering any resulting Master Agreement(s).

Master Agreement means the underlying agreement executed by and between the Lead State, acting on behalf of the NASPO ValuePoint program, and the Contractor, as now or hereafter amended.

NASPO ValuePoint is the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint, a 501(c)(3) limited liability company that is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports as well as other contract administration functions as assigned by the Lead State.

Order or Purchase Order means any purchase order, sales order, contract or other document used by a Purchasing Entity to order the Products.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity; however, a Participating State listed in the Request for Proposal is not required to participate through execution of a Participating Addendum.

Product means any equipment, software (including embedded software), documentation, service or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Products, supplies and services, and products and services are used interchangeably in these terms and conditions.

Purchasing Entity means a state (as well as the District of Columbia and U.S territories), city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, that issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

NASPO ValuePoint Program Provisions

3. Term of the Master Agreement

a. The initial term of this Master Agreement is for Five (5) years. This Master Agreement may be extended beyond the original contract period for up to Five (5) additional years at the Lead State's discretion and by mutual agreement and upon review of requirements of Participating Entities, current market conditions, and Contractor performance. An awarded contract have a co-terminus expiration with existing contracts to allow for ease of administration.

b. The Master Agreement may be extended for a reasonable period of time in adherence to the Utah Procurement Code, if in the judgment of the Lead State a follow-on, competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection shall not be deemed to limit the authority of a Lead State under its state law otherwise to negotiate contract extensions.

4. Amendments

The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.

5. Participants and Scope

a. Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political

subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts are subject to the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

c. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating Entities who are states are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating Entities who are states incur no financial obligations on behalf of other Purchasing Entities. Contractor shall email a fully executed PDF copy of each Participating Addendum to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases.

d. NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint, is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

e. Participating Addenda shall not be construed to amend the following provisions in this Master Agreement between the Lead State and Contractor that prescribe NASPO ValuePoint Program requirements: Term of the Master Agreement; Amendments; Participants and Scope; Administrative Fee; NASPO ValuePoint Summary and Detailed Usage Reports; NASPO ValuePoint Cooperative Program Marketing and Performance Review; NASPO ValuePoint eMarketCenter; Right to Publish; Price and Rate Guarantee Period; and Individual Customers. Any such language shall be void and of no effect.

f. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the consent to participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

g. **Resale.** "Resale" means any payment in exchange for transfer of tangible goods, software, or assignment of the right to services. Subject to any specific conditions included in the solicitation or Contractor's proposal as accepted by the Lead State, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products (the definition of which includes services that are deliverables). Absent any such condition or explicit permission, this

limitation does not prohibit: payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

6. Administrative Fees

a. The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of 0.25% accounts no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on all sales of products and services for both Corporate/Government Responsible (CRU) (less any charges for taxes or shipping). The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

b. Additionally, some states may require an additional fee be paid directly to the state only on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee in subsection 6a shall be based on the gross amount of all sales (less any charges for taxes or shipping) at the adjusted prices (if any) in Participating Addenda.

7. NASPO ValuePoint Summary and Detailed Usage Reports

In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at <http://calculator.naspovaluepoint.org>. Any/all sales made under this Master Agreement shall be reported as cumulative totals by state for Government Responsible accounts. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than thirty (30) days following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data using the format provided in Attachment J. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-ROM, flash drive or other method as determined by the Lead State and NASPO

ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, **social security numbers or any other numerical identifier**, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any Participating Addendum roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due thirty (30) days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

8. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

- c. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.
- d. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.
- e. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, cancel the Master Agreement pursuant to section 28, or not exercise an option to renew, when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. Cancellation based on nonuse or under-utilization will not occur sooner than one year after award (or execution if later) of the Master Agreement. This subsection does not limit the discretionary right of either the Lead State or Contractor to cancel the Master Agreement pursuant to section 28 or to terminate for default pursuant to section 30.
- f. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

9. NASPO ValuePoint eMarket Center

- a. In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. (doing business as JAGGAER) whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.
- b. The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provide customers information regarding the Contractors website and ordering information. The Contractor is required at a minimum to participate in the eMarket Center through Ordering Instructions.
- c. At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that

the Contractor would like the customer to have.

10. Right to Publish

Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan. The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

11. Price and Rate Guarantee Period

All prices and rates must be guaranteed for the initial term of the Master Agreement. Following the initial Master Agreement period, any request for price or rate adjustment must be for an equal guarantee period, and must be made at least (90 Days) days prior to the effective date. Requests for price or rate adjustment must include sufficient documentation supporting the request. Any adjustment or amendment to the Master Agreement shall not be effective unless approved by the Lead State. No retroactive adjustments to prices or rates will be allowed.

12. Individual Customers

Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

Administration of Orders

13. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. Purchasing Entities may define entity or project-specific requirements and informally compete the requirement among companies having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity's rules and policies. The

Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin work without a valid Purchase Order or other appropriate commitment document under the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

- (1) The services or supplies being delivered;
- (2) The place and requested time of delivery;
- (3) A billing address;
- (4) The name, phone number, and address of the Purchasing Entity representative;
- (5) The price per hour or other pricing elements consistent with this Master Agreement and the contractor's proposal;
- (6) A ceiling amount of the order for services being ordered; and
- (7) The Master Agreement identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration, cancellation or termination of this Master Agreement, or otherwise inconsistent with its terms. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any

such indefinite delivery order agreement.

14. Shipping and Delivery

a. The prices are the delivered price to any Purchasing Entity. All deliveries shall be F.O.B. destination, freight pre-paid, with all transportation and handling charges paid by the Contractor. Responsibility and liability for loss or damage shall remain the Contractor's until final inspection and acceptance when responsibility shall pass to the Purchasing Entity except as to latent defects, fraud and Contractor's warranty obligations. The minimum shipment amount, if any, will be found in the special terms and conditions. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an Order to be shipped without transportation charges that is back ordered shall be shipped without charge.

b. All deliveries will be "Inside Deliveries" as designated by a representative of the Purchasing Entity placing the Order. Inside Delivery refers to a delivery to other than a loading dock, front lobby, or reception area. Specific delivery instructions will be noted on the order form or Purchase Order. Any damage to the building interior, scratched walls, damage to the freight elevator, etc., will be the responsibility of the Contractor. If damage does occur, it is the responsibility of the Contractor to immediately notify the Purchasing Entity placing the Order.

c. All products must be delivered in the manufacturer's standard package. Costs shall include all packing and/or crating charges. Cases shall be of durable construction, good condition, properly labeled and suitable in every respect for storage and handling of contents. Each shipping carton shall be marked with the commodity, brand, quantity, item code number and the Purchasing Entity's Purchase Order number.

15. Laws and Regulations

Any and all Products offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

16. Inspection and Acceptance

a. Where the Master Agreement or an Order does not otherwise specify a process for inspection and Acceptance, this section governs. This section is not intended to limit rights and remedies under the applicable commercial code.

b. All Products are subject to inspection at reasonable times and places before Acceptance. Contractor shall provide right of access to the Lead State, or to any other authorized agent or official of the Lead State or other Participating or Purchasing Entity, at reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance requirements under this Master Agreement. Products that do not meet specifications may be rejected. Failure to reject upon receipt, however, does not relieve the contractor of liability for material (nonconformity that substantially impairs value) latent or hidden defects subsequently

revealed when goods are put to use. Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which Acceptance is revoked.

c. If any services do not conform to contract requirements, the Purchasing Entity may require the Contractor to perform the services again in conformity with contract requirements, at no increase in Order amount. When defects cannot be corrected by re-performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and reduce the contract price to reflect the reduced value of services performed.

d. The warranty period shall begin upon Acceptance.

e. Acceptance Testing may be explicitly set out in a Master Agreement to ensure conformance to an explicit standard of performance. Acceptance Testing means the process set forth in the Master Agreement for ascertaining that the Product meets the standard of performance prior to Acceptance by the Purchasing Entity. If Acceptance Testing is prescribed, this subsection applies to applicable Products purchased under this Master Agreement, including any additional, replacement, or substitute Product(s) and any Product(s) which are modified by or with the written approval of Contractor after Acceptance by the Purchasing Entity. The Acceptance Testing period shall be thirty (30) calendar days or other time period identified in this Master Agreement or the Participating Addendum, starting from the day after the Product is delivered or, if installed, the day after the Product is installed and Contractor certifies that the Product is ready for Acceptance Testing. If the Product does not meet the standard of performance during the initial period of Acceptance Testing, Purchasing Entity may, at its discretion, continue Acceptance Testing on a day-to-day basis until the standard of performance is met. Upon rejection, the Contractor will have fifteen (15) calendar days to cure the standard of performance issue(s). If after the cure period, the Product still has not met the standard of performance, the Purchasing Entity may, at its option: (a) declare Contractor to be in breach and terminate the Order; (b) demand replacement Product from Contractor at no additional cost to Purchasing Entity; or, (c) continue the cure period for an additional time period agreed upon by the Purchasing Entity and the Contractor. Contractor shall pay all costs related to the preparation and shipping of Product returned pursuant to the section. No Product shall be deemed Accepted and no charges shall be paid until the standard of performance is met. The warranty period shall begin upon Acceptance.

17. Payment

Payment after Acceptance is normally made within 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance, unless a different late payment amount is specified in a Participating Addendum, Order, or otherwise prescribed by applicable law. Payments will be

remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

18. Warranty

Warranty provisions govern where specified elsewhere in the documents that constitute the Master Agreement; otherwise this section governs. The Contractor warrants for a period of one year from the date of Acceptance that: (a) the Product performs according to all specific claims that the Contractor made in its response to the solicitation, (b) the Product is suitable for the ordinary purposes for which such Product is used, (c) the Product is suitable for any special purposes identified in the solicitation or for which the Purchasing Entity has relied on the Contractor's skill or judgment, (d) the Product is designed and manufactured in a commercially reasonable manner, and (e) the Product is free of defects. Upon breach of the warranty, the Contractor will repair or replace (at no charge to the Purchasing Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

19. Title of Product

Upon Acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Product free and clear of all liens, encumbrances, or other security interests. Transfer of title to the Product shall include an irrevocable and perpetual license to use any Embedded Software in the Product. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license shall be at no additional cost or charge to either Purchasing Entity or Purchasing Entity's transferee.

20. License of Pre-Existing Intellectual Property

Contractor grants to the Purchasing Entity a nonexclusive, perpetual, royalty-free, irrevocable, license to use, publish, translate, reproduce, transfer with any sale of tangible media or Product, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual Property"). The Contractor shall be responsible for ensuring that this license is consistent with any third party rights in the Pre-existing Intellectual Property.

General Provisions

21. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of

this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than \$1 million per occurrence/\$2 million general aggregate;

(2) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

c. Contractor shall pay premiums on all insurance policies. Contractor shall provide notice to a Participating Entity who is a state within five (5) business days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that written notice of cancellation shall be delivered in accordance with the policy provisions, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, other state Participating Entities' rights and Contractor's obligations are the same as those specified in the first sentence of this subsection except the endorsement is provided to the applicable state.

e. Contractor shall furnish to the Lead State copies of certificates of all required insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. Failure to provide evidence of coverage may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

22. Records Administration and Audit

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and Orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of five (5) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, or such longer period as is required by the Purchasing Entity's state statutes, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or Orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

23. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity or Purchasing Entity's clients. Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

e. The rights granted Purchasing Entities and Contractor obligations under this section shall also extend to the cooperative's Confidential Information, defined to include Participating Addenda, as well as Orders or transaction data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line item descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead State, a Participating State, or any governmental entity exercising an audit, inspection, or examination pursuant to section 23. To the extent permitted by law, Contractor shall notify the Lead State of the identify of any entity seeking access to the Confidential Information described in this subsection.

24. Public Information

This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Assignment/Subcontracts

a. Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

b. The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint and other third parties.

26. Changes in Contractor Representation

The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel managing the Master Agreement in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

27. Independent Contractor

The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

28. Cancellation

Unless otherwise stated, this Master Agreement may be canceled by either party upon 60 days written notice prior to the effective date of the cancellation. Further, any Participating Entity may cancel its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision shall not affect the rights and obligations attending orders outstanding at the time of cancellation, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Cancellation of the Master Agreement due to Contractor default may be immediate.

29. Force Majeure

Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, unusually severe weather, other acts of God, or war which are beyond that party's reasonable control. The Lead State may terminate this Master Agreement after determining such delay or default will reasonably prevent successful performance of the Master Agreement.

30. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or
- (4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or
- (5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, the Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 15 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and the Lead State shall have the right to exercise any or all of the following remedies:

- (1) Exercise any remedy provided by law; and
- (2) Terminate this Master Agreement and any related Contracts or portions thereof; and
- (3) Impose liquidated damages as provided in this Master Agreement; and
- (4) Suspend Contractor from being able to respond to future bid solicitations; and
- (5) Suspend Contractor's performance; and
- (6) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and shall have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Unless otherwise specified in a Purchase Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

31. Waiver of Breach

Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

32. Debarment

The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

33. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO Cooperative Purchasing Organization LLC (doing business as NASPO ValuePoint), the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees, from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO Cooperative Purchasing Organization LLC (doing business as NASPO ValuePoint), the Lead State, Participating Entities, Purchasing Entities, along with their officers and employees ("Indemnified Party"), from and against claims, damages or causes of action

including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

34. No Waiver of Sovereign Immunity

In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This section is also not a waiver by the state of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

35. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State. The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; a Participating State if a named party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

36. Assignment of Antitrust Rights

Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

37. Contract Provisions for Orders Utilizing Federal Funds

Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating

Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this Master Agreement.

38. Leasing or Alternative Financing Methods

The procurement and other applicable laws of some Purchasing Entities may permit the use of leasing or alternative financing methods for the acquisition of Products under this Master Agreement. Where the terms and conditions are not otherwise prescribed in an applicable Participating Addendum, the terms and conditions for leasing or alternative financing methods are subject to negotiation between the Contractor and Purchasing Entity.



NASPO
ValuePoint

MA3696

Wireless Data, Voice, and Accessories

Attachment B

Scope of Work

Section 1: General

1.1 Background

The State of Utah Division of Purchasing and General Services (“Lead State”) is requesting proposals for Wireless Data, Voice and Accessories in furtherance of the NASPO ValuePoint Cooperative Purchasing Program. The purpose of this Request for Proposal (RFP) is to establish Master Agreements with qualified Contractors and refresh the existing Master Agreements for Wireless Data, Voice, and Accessories for all Participating States in Award Category 3 (IOT offerings). The objective of this RFP is to obtain best value, and in some cases achieve more favorable pricing, than is obtainable by an individual state or local government entity because of the collective volume of potential purchases by numerous state and local government entities. The Master Agreement(s) resulting from this procurement may be used by state governments (including departments, agencies, institutions), institutions of higher education, political subdivisions (i.e., colleges, school districts, counties, cities, etc.), the District of Columbia, territories of the United States, and other eligible entities subject to approval of the individual chief procurement official and compliance with local statutory and regulatory provisions. The initial term of the master agreement shall be conterminous with the current Master Agreements which are 5 (Five) years with renewal provisions for an additional 5 (Five) as outlined in Section 3 of the NASPO ValuePoint Master Terms and Conditions (Attachment A).

1.2 Order of precedence

Per the NASPO ValuePoint Master Terms and Conditions, Participating Addenda (called “PA”) will have precedence over the Master Agreement within the participating jurisdiction.

1.3 Green Awards

End users of the Master Agreements that derive from this solicitation may have requirements to purchase products and services that adhere best practices of sustainability and environmental consciousness. Contractors should anticipate addressing these needs as they arise in the Participating Addendum process.

1.4 E-Rate

To the extent the services offered are subject to the E-rate discount program, all award Contract Vendors must commit to participation in the Federal Communication Commission's E-rate discount program established under authority of the Federal Telecommunications Commission Act of 1996. Participation in, and implementation of, this program must be provided without the addition of any service or administration fee by the Contract Vendor.

1.5 Net Neutrality

Recent changes by the Federal Communications Commission in their rules related to the issue of Net Neutrality have increased state’s interest in promulgating their own law, rule and policies on this topic. This solicitation will have no requirements related to Net Neutrality for the Master Agreements. It is anticipated, that this issue will be pertinent in the Participating Addendum process.

Section 2: Category of Award

2.0 Overview of Award Category

The products and services for this solicitation will be awarded in 1 (one) category. This Category will be referred to as “Category 3” to keep the category consistent with the original solicitation for wireless data, voice and accessories (CJ18012):

Category 3- Turnkey Wireless and IoT Solutions that are offered as a product: This category includes any of the wireless or IoT solutions or applications being offered as a complete product by the cellular wireless carriers or any other Contractor(s).

2.1 Category 3 – Internet of Things and other Turnkey Wireless Applications

2.1.1 Definitions

Contractor The signing party of this Master Agreement.

Turnkey Wireless Solution For the purposes of this solicitation a Turnkey Wireless Solution is an integrated, on premise or hybrid system that includes three broad elements:

- End Points physical objects (things like sensors, cameras, end point devices, etc.) that contain embedded technology to sense or interact with their internal state or external environment and the ability to communicate with a remote application
- Network Services a wireless communication network providing M2M communication services or some other method of data transport connecting the dedicated physical objects with;
- Back Office Systems applications and central or back end systems (servers, software, operating systems, storage, etc.).

2.1.2 Turnkey Wireless Solutions

A Contractor shall fully disclose what is included in the Turnkey Wireless Solutions, including all operational components, training, services, equipment, licenses, third party agreements, any and all fees and performance guarantees.

Turnkey Wireless Solutions Single Contract The provider offering a Turnkey Wireless Solutions may utilize subcontractors and partners to provide various elements of the system, but the system including all licensing rights will be covered by a single contract between the end user that purchases the system and the provider who is awarded a master agreement for this category of award.

Limited Related Service The provider shall provide support services as needed to install, maintain and enhance the system over the life of the system. These Limited Related Services shall be included in the system pricing. Installation services may be capped in proportion to the project at hand. The Proposal shall describe all related services that are included in the Turnkey Wireless System. The purchasing entity shall have the option to purchase additional services at pricing offered by the proposer and provide an hourly rate related to the project for the Additional Consulting or Integration Services.

Additional Consulting or Integration Services

- a. The purchasing entity shall have the ability to purchase consulting or integration services from the provider.
- b. Consulting Services – In Category 3, “Consulting Service” means planning, assessment and other professional consulting services provided by the Contractor related to the public entities planning, design, assessing, operating or maintaining an IoT solution.
- c. Additional Services – In Category 3, “Integration Service” means the process of making new IoT devices, data, platforms and applications, as well as existing IT assets (for example, business applications, data, mobile, SaaS and legacy systems) work well together in the context of implementing end-to-end IoT business solutions. Integration services are not part of turnkey

system or limited related service, but may be acquired from the provider or from a separate integration service provider at the sole discretion of the purchasing entity.

Limited Related Service and Additional Consulting or Integration Services will be billed at an Hourly rate will be included on the Cost Sheet (Attachment C) and will be included in the Master Agreement. The Hourly rate will be a blended rate and will encompass all related cost for these additional services.

2.1.3 Category 3 Subcategories of Award

See Attachment V for Category 3 Subcategory Definitions.

Right to Refresh

This category of master agreements (Turnkey Wireless Solutions) may be reopened and refreshed at the sole discretion of the Lead State at any time. The refresh may allow additional Turnkey Wireless Solutions offering in the broad scope or by specifically identified sub categories. The Lead State reserves the right to change the methodology for award for all or any subcategories at the time of the refresh/reopen of the solicitation. Awards for Award Category 3 in any refresh solicitation will be given the same contract term as the initial award.

Data Protection

The provider shall:

- a. Specify the best available standards-based encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.
- b. Describe whether or not it is willing to sign relevant and applicable agreements that may be necessary to protect data with a Purchasing Entity.
- c. Describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement.
- d. Specify its data disposal procedures, policies and destruction confirmation process

Subcontractors

Providers must explain for each Turnkey Wireless Solutions offered if they intend to provide it directly or through the use of Subcontractors. Any Subcontractor that a Provider chooses to use in fulfilling the requirements of the solicitation must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the solutions provided in this category.

- a. Contractor must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.
- b. If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP.

- c. Include a description of how the Contractor will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

2.1.4 Security For each Turnkey Wireless Solutions proposed include both a security disclosure statement.

Contractors for Award Category 3 have submitted answers to Attachment S- Security Disclosure Statement.

2.1.5 Client Infrastructure Impact and Support

Contractors will be willing to provide a description of the Impact and Support on End User infrastructure upon request Assessment what impacts the Turnkey Wireless application will have on the infrastructure used by purchasing entity, including the client's network, data storage and client owned and operated endpoints before installation. Contractor will at the time of purchase identify any support required by the purchasing entity to support the proposed Turnkey Wireless Solutions.

2.1.6 Client Infrastructure and Support

Unless the purchasing entity waives the requirement, the Contractor shall provide a description of the Impact and Support on the End User infrastructure. This shall include an assessment of impacts the Turnkey Wireless application will have on the infrastructure used by purchasing entity, including the client's network, data storage and client owned and operated endpoints before installation. The description shall also identify any resources required by the purchasing entity to support the proposed Turnkey Wireless Solutions.

2.1.7 Pricing Requirements

Cost Sheet

See Attachment C for details for Award Category 3.

No other Terms and Conditions, End User Agreements, or any other terms will be offered with the new product or service unless it is included in the Master Agreement at formation or by Amendment.

Section 3: Award Criteria for Categories of Award

3.1 Category 3: Turnkey Wireless and IoT Solutions

The Minimum Mandatory Requirements and Technical Scorable Criteria in this section were used for the award of this contract.

3.1.1 Minimum Mandatory Requirements

3.3.1.1 General Minimum Mandatory Requirements

Reporting Requirements - Contractor will adhere to reporting requirements listed in Section 6 and Attachments J as applicable.

Dedicated NASPO ValuePoint Representation - Contractor must designate centralized point(s) of contact for sales, customer service escalation and contract administration. These roles can be held by one individual or up to three different individuals, provided all points of contact report to the same supervisor or manager within the Contractor's organization.

Financial Stability Attestation- Attachment R Contractor must submit a filled out Attachment R Financial Stability Form. Including a Dun and Bradstreet "DUNS" rating and report.

Data Ownership Attestation **Unless otherwise specifically agreed to by the Purchasing Entity, the Purchasing Entity will own all right**, title and interest in its data that is related to the Services provided by this Master Agreement. The Provider shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course system operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

b. Provider and any Subcontractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

3.3.1.2 Category Specific Minimum Mandatory requirements

Security Disclosure Statement Contractor must fill out the attached Security Disclosure Statement, Attachment S.

Award Category 3 Questionnaire Contractor must fill out the attached Award Category 3 Questionnaire, Attachment T.

Client Questionnaire Contractor must have clients of their choice fill out the attached Attachment Q, and include it with their proposal.

Complete Turnkey Wireless Solution For solutions offered in this Category, the Contractor will be responsible for obtaining all of the required components (endpoints, network services, back-office processing, network management, etc.), testing to ensure functionality and

interoperability, ensuring security of the solution, and provide installation, project management for the overall solution delivered and serve as the single billing entity.

3.3.2 Technical Scorable Criteria

3.3.2.1 General Technical Scorable Criteria

Reporting Contractor will be scored based on their demonstrated reporting capabilities to end users, NASPO ValuePoint, and the Lead State. Flexibility and customizability in reporting is desired.

Company information Contractor will be scored based on the perceived capability, experience and expertise of their firm. Information that is not limited to but may include:

- a. Employee number and expertise
- b. Years of experience
- c. Infrastructure
- d. Coverage
- e. Financial health of company

Customer Service and escalation Contractor will describe how it will address customer service and escalation of issues. Committee will score based on the perceived effective customer service plan and any other related services offered.

3.3.2.2 Category Specific Technical Scorable Criteria

Turnkey Offerings Contractor will be scored based on their demonstrated value and capability of their turnkey offering.

Description of Turnkey Planning and Process Contractor will be scored based on the customer service they offer in this category. Factors to be considered is not limited to, but may include:

- a. Dedicated Point of Contact
- b. Training offered to NVP
- c. Escalation Plan

Service Factors Contractor will be scored based on:

- a. Description of related services included in Turnkey Solution
- b. Experience and qualifications of related service providers
- c. Description of Additional Integration and Consulting Services provided
- d. Experience and qualifications of Additional Integration and Consulting Services

References Contractor will be scored based customer/end user responses to the Client Questionnaire, Attachment Q.

Training Training will be scored based on training plan in this category:

- a. Pre installation training
- b. Operational training
- c. Ongoing Training

Security Contractor will be scored on their services, and offerings related to security. Items to be considered:

- a. Security Disclosure Statement (Attachment S)
- b. Data ownership and control
- c. Infrastructure Impact and Support provisions including provisions taken to ensure that failure of the turnkey solution will not impact the underlying operations

3.3.3 Cost Criteria (See Attachment C)

Section 4: Adding New Products and Services

The Lead State anticipates establishing a process for regular communication with contractors and addition of new products and services. Addition of new products will be treated differently based on which category of award covers the product or service.

4.1 General Requirements

The Lead State, along with the sourcing committee of this Solicitation will review and add new products and services to the Master Agreements outlined below. The Lead State reserves the right to modify this process to ensure open, transparent and reasonable review of proposed new products and services.

4.4 New Products added under Award Category 3

For new products under Award Category 3, Contractors must submit a request to the Lead State and sourcing team for consideration using Attachment N. All new products under Award Category 3 will be allowed only through amendment of the Master Agreements that result from this solicitation.

After consultation with the sourcing team, the Lead State may choose to include the new product under the Master Agreements by amendment. The Contractor will provide an updated Attachment G at the next quarterly update for public distribution.

4.4.1 New Product Request Form

The New Product Request form will be submitted to the Lead State to request any new products or services under Award Category 3(See Attachment M).

Proposed additional terms and conditions, end user agreements or related materials to be used with the new product must be included with the New Product Request form to be considered for addition to the Master Agreement. Terms and Conditions for additional products/services may be negotiated by the Lead State before addition.

4.4.2 New Product Request Log

All new added products and services under Award Category 3 will be included on Attachment N, Request Log sheet that will include Lead State recommendations and observations. This log will be included in the contract file and will be available for public view.

4.4.3 Quarterly Amendments

The Lead State expects to conduct quarterly amendments of the Master Agreement to add new products and services under Award Category 3. The Lead State reserves the right to amend, or not amend the Master Agreement at any time.

Terms and Conditions not included in the addition of new products for Award Category 3 will not be part of any agreement with end users. Contractors will not present end users with only the Terms and Conditions agreed to by the parties in the Master Agreement Amendment.

4.4.4 Terms and Conditions Compliance with Master Agreement

All Products offered under Award Category 3 shall comply fully with all applicable Federal and State laws and regulations. The Order of Precedence clause in the NASPO ValuePoint Master Agreement Terms and Conditions and/or Participating Addendum will control in the event of any conflict between the NASPO ValuePoint Master Agreement and/or Participating Addendum and the Product Terms and Conditions. Any third-party product provider must agree to the Master Agreement Terms and Conditions.

4.6 Quarterly Call/Meeting

The Lead State expects to have a call with contractors every quarter to discuss the status of the contracts, discuss proposed new products and services, and any other issues that may arise regarding the contract. These calls/meetings will be scheduled at mutually agreed upon times.

4.7 Terms and Conditions Compliance with Master Agreement

Any and all Products offered and furnished under any award category shall comply fully with all applicable Federal and State laws and regulations. The Order of Precedence clause in the NASPO ValuePoint Master Agreement Terms and Conditions and/or Participating Addendum will control in the event of any conflict between the NASPO ValuePoint Master Agreement and/or Participating Addendum and the Product Terms and Conditions. Any third-party product provider must agree to the Master Agreement Terms and Conditions.

Section 6: Reporting

6.1 General Requirements

6.1.1 Reporting shall be provided in the format required by NASPO ValuePoint:

6.1.1.3 Attachment J (Award Category 3)

6.1.2 Attachment G: Contract Coverage Attachment

Contractors under the Master Agreement that results from this contract will submit quarterly Attachment G to the Lead State. This attachment is intended to encapsulate the plans, services and offerings of the contractor. This would include any legacy and current offerings, including the plans entered on Attachment C. (anything that would be covered by the Master Agreement).

Attachment G must be submitted by Contractors awarded Award Category 3.

6.1.3 Individual participating entities may request specific equipment sales summaries, which shall be provided at no cost.

Upon request, provide reporting elements and/or management reports related to usage for services that are available and would optimize the participating entity's ability to assess utilization and cost.

Be able to provide custom reports as may be requested by individual participating entities. Describe in general, the level of sophistication and complexity, custom usage report data that you can provide to the participating entities. Vendors should provide a sample report with their proposal.

Upon request, provide subscribers with usage reports which include full itemization of call details (such as the information on the Contractor's standard bill for consumer accounts) to enable verification of usage including: (1) call date, call number call length, call time, and (2) plan cost, per minute charges, overage cost, additional features charges and other fees, etc.

6.2 Quarterly Call/Meeting

Contractors must be available for a quarterly meeting by phone, video conference, or in person to discuss contract concerns, developments and any upcoming additional products or services related to reporting.

6.4 Usage Reports (Other States)

Other States and participating entities may have alternate reporting requirements and will be addressed by their Participating Addendum.

Section 8: Administration of Contracts

8.1 Quarterly Amendment

The Lead State anticipates it will provide for regular quarterly amendments to the Master Agreement if there is a need to add new products or services. (Section 4). The Lead State at its discretion may elect to amend the Master Agreement at any time.

8.2 Quarterly Call

The Lead State and sourcing team intend to hold quarterly calls to facilitate new products/services, discuss the administration of the Master Agreements, and all other applicable aspects of the master agreement.

8.3 Annual Meeting

Contractors must be available for an annual meeting in person to discuss continuing administration of the contract. The Lead State anticipates meeting once a year in person to facilitate more in depth communication. The location of in-person meetings will be in The Salt Lake City area, or elsewhere at the discretion of the Lead State.

8.4 Published Documents

The Lead State intends to publish all new product/service request forms, new product logs, and any sourcing committee recommendations and notes related for reference. End users may use these documents to aid in their purchasing decisions.

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets

Category 3A: Fleet Management Costsheets

VENDOR

US Cellular

Monthly Recurring Cost

Description	minimum quantity of vehicles	monthly fee	total annual cost (qty x fee x 12)	OFFEROR NOTES Describe plan attributes and characteristics per the instructions*.
Basic Fleet Management	10	\$13.48		GPS Trackit Fleet Manager- Provide real-time vehicle-based GPS tracking and management system including device to be either hardwired under or Plug and Play (PnP) into the OBDII port with 3MB pooled data connectivity plan
	100	\$13.48		
	500	\$13.48		
	1000	\$13.48		
	5000	\$13.48		
Total Annual Recurring Cost				

Service Requirements

Description	requirements
Basic Fleet Management	*Solution to track, monitor & dispatch vehicles while collecting information on vehicle location & operation *must have option to connect to vehicle's On Board Diagnostic-II (OBD-II) port *Ability to monitor vehicle location *Provide location-based vehicle dispatch support *Collect information on driver performance *Real time and historical reporting via secure, centralized portal *Ability to set up alerts based on customer devined parameters

Installation & Set Up Costs

Description	minimum quantity of vehicles	cost per vehicle	Total Set Up Cost	OFFEROR NOTES Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10	\$85.00		There is no activation fee and devices are plug in play self install
	100	\$85.00		
	500	\$77.00		
	1000	\$77.00		
	5000	\$77.00		
Total Installation and Set Up Cost				

Installation & Set Up Requirements

Description	requirements
Installation, Set Up and Basic System Administrator Training	*Set up and configuration of customer's instance in provider's hosted environment. *install each device in vehicle and connect to OBD-II

Scorable Cost

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheet

Category 3A: Fleet Management Costsheet

VENDOR

US Cellular

Monthly Recurring Cost

Description	minimum quantity of vehicles	monthly fee	total annual cost (qty x fee x 12)	OFFEROR NOTES Describe plan attributes and characteristics per the instructions*.
Basic Fleet Management	10	\$11.95		READY FLEET allows for any fleet manager to operate and track their vehicles efficiently with minimal equipment and maintenance. The intuitive platform allows for detailed reporting and insight to the 3 main “pillars” of fleet management: location/geotracking, maintenance/diagnostics and driver behavior. Unique to the platform is the ability to tether a driver’s phone to the vehicle via the cloud and monitor distracted driving behavior (e.g. texting, app use) while behind the wheel of a state-owned vehicle with 25MB Pooled data connectivity plan
	100	\$11.95		
	500	\$11.95		
	1000	\$11.25		
	5000	\$10.55		
Total Annual Recurring Cost				

Service Requirements

Description	requirements
Basic Fleet Management	*Solution to track, monitor & dispatch vehicles while collecting information on vehicle location & operation *must have option to connect to vehicle's On Board Diagnostic-II (OBD-II) port *Ability to monitor vehicle location *Provide location-based vehicle dispatch support *Collect information on driver performance *Real time and historical reporting via secure, centralized portal *Ability to set up alerts based on customer devined parameters

Installation & Set Up Costs

Description	minimum quantity of vehicles	cost per vehicle	Total Set Up Cost	OFFEROR NOTES Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10	\$158.00		Cost of OBDII Device
	100	\$158.00		
	500	\$158.00		
	1000	\$158.00		
	5000	\$158.00		
Total Installation and Set Up Cost				

Installation & Set Up Requirements

Description	requirements
Installation, Set Up and Basic System Administrator Training	*Set up and configuration of customer's instance in provider's hosted environment. *install each device in vehicle and connect to OBD-II

Scorable Cost

\$0.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheet

Category 3A: Fleet Management Costsheet

VENDOR

US Cellular

Monthly Recurring Cost

Description	minimum quantity of vehicles	monthly fee	total annual cost (qty x fee x 12)	OFFEROR NOTES Describe plan attributes and characteristics per the instructions*.
Basic Fleet Management	10	\$13.48		MiFleet Fleet and Asset management solutions including, OBDII plug and play, Three wire covert solution, IP6X rated solutions for heavy duty equipment, and ELD solutions with 3MB pooled data connectivity plan
	100	\$13.48		
	500	\$13.48		
	1000	\$12.11		
	5000	\$10.73		
Total Annual Recurring Cost				

Service Requirements

Description	requirements
Basic Fleet Management	*Solution to track, monitor & dispatch vehicles while collecting information on vehicle location & operation *must have option to connect to vehicle's On Board Diagnostic-II (OBD-II) port *Ability to monitor vehicle location *Provide location-based vehicle dispatch support *Collect information on driver performance *Real time and historical reporting via secure, centralized portal *Ability to set up alerts based on customer devined parameters

Installation & Set Up Costs

Description	minimum quantity of vehicles	cost per vehicle	Total Set Up Cost	OFFEROR NOTES Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10	\$145.00		Cost of OBDII Device
	100	\$145.00		
	500	\$145.00		
	1000	\$145.00		
	5000	\$145.00		
Total Installation and Set Up Cost				

Installation & Set Up Requirements

Description	requirements
Installation, Set Up and Basic System Administrator Training	*Set up and configuration of customer's instance in provider's hosted environment. *install each device in vehicle and connect to OBD-II

Scorable Cost

\$0.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets				
Category 3B: Mobile Device Management Costsheets				
VENDOR		US Cellular		
Monthly Recurring Cost				
Description	minimum quantity of licenses	monthly fee	total annual cost (qty x fee x 12)	OFFEROR NOTES Describe plan attributes and characteristics per the instructions*.
Basic Mobile Device Management cost per device	10	\$4.00		Mobile Device Management for iOS, Android, Windows, macOS Mobile App Management for iOS, Android, Windows, macOS Patch and Update Management Identity Management Advisor Container App Expense Management
	100	\$4.00		
	500	\$4.00		
	1000	\$4.00		
Total Annual Recurring Cost				
Service Requirements				
Description		requirements		
Basic Mobile Device Management		*central control to enroll, configure, secure, monitor and manage all enrolled devices (iOS, Android, Blackberry, Windows) *Ability to configure and update devices over-the-air *Ability to push and update custom apps to devices over-the-air *Enforce security and compliance policies *Secure Mobile Access to corporate resources *Provide Secure Container for corporate apps and data on each device *Ability to remote wipe entire device and / or only apps and data in secure container		
Installation & Set Up Costs				
Description	minimum quantity of licenses		Total Set Up Cost	OFFEROR NOTES Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10			
	100			
	500			
	1000			
Total Installation and Set Up Cost			\$0.00	
Installation & Set Up Requirements				
Description		requirements		
Installation, Set Up and Basic System Administrator Training		*Set up and configuration of customer's instance in provider's hosted environment. *At least one remote meeting with customer's designated system administrator to complete set up and provide knowledge transfer.		

Scorable Cost	

Consultative Hourly Rate (this rate will be included in the contract)	\$0.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets				
Category 3B: Mobile Device Management Costsheet				
VENDOR			US Cellular	
Monthly Recurring Cost				
Description	minimum quantity of licenses	monthly fee		OFFEROR NOTES Describe plan attributes and characteristics per the instructions*.
Basic Mobile Device Management cost per device	10	\$6.00		ScaleFusion is a cloud based Device Management solution that does much more than just managing and securing Employee-Owned (BYOD and/or Company-Owned devices. Unlocking the true Enterprise Mobility potential with finesse (BlackBerry® is not applicable)
	100	\$4.50		
	500	\$3.00		
	1000	\$2.25		
Total Annual Recurring Cost				
Service Requirements				
Description		requirements		
Basic Mobile Device Management		*central control to enroll, configure, secure, monitor and manage all enrolled devices (iOS, Android, Blackberry, Windows) *Ability to configure and update devices over-the-air *Ability to push and update custom apps to devices over-the-air *Enforce security and compliance policies *Secure Mobile Access to corporate resources *Provide Secure Container for corporate apps and data on each device *Ability to remote wipe entire device and / or only apps and data in secure container		
Installation & Set Up Costs				
Description	minimum quantity of licenses		Total Set Up Cost	OFFEROR NOTES Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10			Usually setup cost is included in the licensing cost but when the volumes of devices go up, the support and the service cost goes up. Hence a flat fee of USD 2500 will be charged when the number of devices crosses 500 and every increment of 1000 devices will attract a one time fee of USD 500 for setup, configuration and activation.
	100			
	500		\$2,500.00	
	1000			The platform is self service and hence client may not require this service.
Total Installation and Set Up Cost				
Installation & Set Up Requirements				
Description		requirements		
Installation, Set Up and Basic System Administrator Training		*Set up and configuration of customer's instance in provider's hosted environment. *At least one remote meeting with customer's designated system administrator to complete set up and provide knowledge transfer.		

Scorable Cost	

Consultative Hourly Rate (this rate will be included in the contract)	\$75.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets
Award Category 3-E Costsheets

Vendor Name:					US Cellular
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	Goldie Field Service Management	Systems that support the management of field service operations typically managing service orders, dispatching technicians, work planning, route optimization, time recording, maintenance data collection/analysis and other related functions.	Our product will take care of Workforce management, Field Service Management and Data collection using mobile forms. The cost remains the same and therefore the client can drastically save on separate solutions and have all data points in one place for ease of operation and access. As a 3-in-1 solution the ability to quickly roll out work allocations and data collection to field personnel will be managed easily using one single dashboard. Forecasting, Budgeting, Planning etc is not available as part of the solution. Basic Data visualization is available and advanced visualization can be enabled by directing data towards tools like Tableau or Qlik, etc	20.00%	30% discount is applicable when minimum number of devices crosses 5000 threshold. Below which a standard 20% discount is provided across slabs which are less than 5000 devices.
				20.00%	

*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.

Consultative Hourly Rate (this rate will be included in the contract)	\$75.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets

Award Category 3-F Costsheets

Vendor Name:

US Cellular

	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	doForms Mobile Data Collection Solution	\$9.95	Standard Package	10.00%	doForms is a highly flexible and scalable mobile data collection solution that provides customers with the ability to quickly build, deploy and collect customized mobile forms. Forms can be as simple or complex as required with a very user intuitive interface. Form capabilities include but not limited to lookup tables, if then else logic, GPS stamps/tracking, email workflow, form forwarding, media capture (audio, images, signatures, sketches, and video), support for offline (store & forward) scenarios, and much more. doForms is easily installed on supported Apple iOS or Google Android mobile devices in minutes with additional support for web-based forms. Mobile forms are auto responsive to any device screen size out of the box with optional customization of scrolling or panning of forms.
	doForms Mobile Data Collection Solution	\$14.95	Advanced Package		
	doForms Mobile Data Collection Solution	\$19.95	Premium Package		
				10.00%	

*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.

Consultative Hourly Rate (this rate will be included in the contract)

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-F Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	Team On The Run SaaS Full plus My Business per user per month fee <u>Mandatory fee - Recurring per user</u>	\$10 per month / user	- My Business process and forms - Secured Messaging - Voice services : PTT & VOIP - Geo-location	10.00%	Includes Team On the Run Full feature & My Business
	Team On The Run SaaS My Business activation <u>Mandatory fee , non-recurring</u>	\$500	Includes My business activation with 1 hour consultation and one custom Mybusiness process template		
	Team On The Run SaaS My Business customized workflow template <u>Optional Fee , non-recurring</u>	\$250	If customer needs Team On The Run services to assists customizing a My Business process template.		
				10.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$187.50				

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets

Award Category 3-F Costsheets

Vendor Name:

US Cellular

	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	Goldie Mobile Data Collection/Mobile Forms	A solution(s) that allow mobile users with cellular-equipped tablets or smartphones to collect data and possibly other information (e.g. pictures, videos, audio notes, locations, etc.), which is then sent over the cellular network to a cloud storage facility from which it can be accessed or downloaded by the customer.	Our product will take care of Workforce management, Field Service Management and Data collection using mobile forms. The cost remains the same and therefore the client can drastically save on separate solutions and have all data points in one place for ease of operation and access. As a 3-in-1 solution the ability to quickly roll out work allocations and data collection to field personnel will be managed easily using one single dashboard. Forecasting, Budgeting, Planning etc is not available as part of the solution. Basic Data visualization is available and advanced visualization can be enabled by directing data towards tools like Tableau or Qlik, etc	20.00%	30% discount is applicable when minimum number of devices crosses 5000 threshold. Below which a standard 20% discount is provided across slabs which are less than 5000 devices.
				20.00%	

*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.

Consultative Hourly Rate (this rate will be included in the contract)	\$75.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-G Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	READY ASSET PRO	Sensor Management	Traffic Managmeent and Intelligent Transport, Energy Conservation Mgmt, Building & Facilities Automation, Health and Human Services	30.00%	100+ Sensors. A Monthly Platform Fee of \$110 per site per use case
				30.00%	
	*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.				
Consultative Hourly Rate (this rate will be included in the contract)	\$0.00				

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-G Costsheets					
Vendor Name:			US Cellular		
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	PARKNAV	On-street & Off-street Parking Informa	Real-time parking availability predicti	25.00%	Data Included in solution
				25.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)					

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets

Award Category 3-H Costsheets

Vendor Name:

US Cellular

	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	Connect Anywhere Monthly Service	The SkyHawk ConnectAnywhere web-based monitoring solution is an enterprise level, cloud based service which facilitates the real-time visibility and management of an organization's valuable assets. The service provides unique asset identification, GPS location and vehicle status integration with sensory information such as plow, spreader, PTO, beacon and brooms.	Four levels of service available: Professional, Express, Lite, and Asset. Providing the features and pricing to meet your business needs. Services are priced per asset, with an unlimited number of users, reports, and usage	15.00%	
				15.00%	

*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.

Consultative Hourly Rate (this rate will be included in the contract)

\$150.00

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-I Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off/ Discount (%)*	Notes
	QPP	\$0	Wireless QoS, Priority, Pre-emption for 4G Data with private dedicated core network infrastructure.	100.00%	
				100.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)					

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheet					
Award Category 3-I Costsheet					
Vendor Name:					
US Cellular					
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	WPS	\$0	Wireless Priority Service	100.00%	Advanced functionality to ensure prioritized voice service availability
				100.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)					

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 3-I Costsheet

Vendor Name:

US Cellular

	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	Team On The Run SaaS Full feature per user per month fee Mandatory fee - Recurring per user	\$6 per month / user	- Secured Messaging - Voice services : PTT & VOIP - Geo-location	10.00%	Includes Team On the Run Full feature
	Video Add-On Streaming / Calling Optional fee - Recurring per user	\$6 per month / user	- Video Calling - Video Streaming		Incremental price add-on per user per month
	Emergency Call/Message / Lone Worker Optional fee - recurring per user	\$2 per month / user	- Emergency call/ Message - Lone Worker protection		Incremental price add-on per user per month
				10.00%	

*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.

Consultative Hourly
Rate (this rate will be
included in the
contract)

\$187.50

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-J Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	ConnectHQ powered by Nokia WING	50	ConnectHQ is a self-service platform enabling business customers to manage connectivity for data-only devices.	100.00%	ConnectHQ powered by Nokia WING is equipped to handle the ever-present IoT reality. That means everything from utility meters, Smartphones, signboards, remote sensors, cameras and appliances are interconnected and need a centralizing system to coordinate their interfacing. ConnectHQ is a Connected Device Platform built for larger scale operations and is especially beneficial for those that do not have an in-house IT department. ConnectHQ can take away barriers to those wanting to maximize IoT solutions for their organization.
				100.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)					

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheet					
Award Category 3-J Costsheet					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	iQ2-Remote Monitoring and Control Industrial IoT Platform.		Remote monitor and control of industrial and municipal assets. Including, but not limited to: Pumps, compressors, generators, water/wastewater infrastructure, utility/energy infrastructure, remote sensors, ITS assets, etc.	10.00%	* Reduced truck-rolls to remote sites and infrastructure - reduces costs and increases safety * Establish state and federal compliance for remote monitoring of disconnected or unmanaged field assets * Provide real-time and historical data analytics to improve operational efficiency and reduce related costs * Provide alerting and alarming to mission critical assets to reduce risk of system failures and costs associated with such failures
				10.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)					

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-M Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off/ Discount (%)*	Notes
	Team On The Run SaaS Full feature per user per month fee Mandatory fee - Recurring	\$6 per month / user	- Secured Messaging - Voice services : PTT & VOIP - Geo-location	10.00%	Includes Team On the Run Full feature
				10.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$187.50				

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-N Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off/ Discount (%)*	Notes
	CyberReef	Private network plus	\$5 /month	10.00%	
	CyberReef	Secure bandwidth manage private VPN	\$5 /month		
	CyberReef	Education CIPA filtering Private network	\$5 /month		Mobile Children's (CIPA) Content Filtering, Cost Management & Security
				10.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$0.00				

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheet					
Award Category 3-N Costsheet					
Vendor Name:			US Cellular		
	Product Name	Product Description	Characteristics of Product	Percentage Off/ Discount (%)*	Notes
	Private Tunneled Virtual Private Network	50	Encrypted traffic, Private Static IP address assignment, GRE over IPSEC tunnels.	100.00%	
				100.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$0.00				

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-O Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	IQ2-Remote Monitoring and Control Industrial IoT Platform.		Remote monitor and control of industrial and municipal assets. Including, but not limited to: Pumps, compressors, generators, water/wastewater infrastructure, utility/energy infrastructure, remote sensors, ITS assets, etc.	10.00%	* Reduced truck-rolls to remote sites and infrastructure - reduces costs and increases safety * Establish state and federal compliance for remote monitoring of disconnected or unmanaged field assets * Provide real-time and historical data analytics to improve operational efficiency and reduce related costs * Provide alerting and alarming to mission critical assets to reduce risk of system failures and costs associated with such failures * The cloud-based application provides real-time insight into asset performance via any web-enabled device or handset decreasing response time to critical field failures. * Highly flexible system allows low-cost and simple integration with existing systems. * Non-proprietary hardware allows for quick availability and competitive costs on off-the shelf hardware across multiple OEM's.
				10.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$150.00				

Configure

Configure

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-O Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	IQ Pulse- Advanced Metering Infrastructure (AMI)		The IQ Pulse IIoT Web portal is a water usage collection database that collects and calculates daily water consumption, as well as provides alarming notification mechanisms for detecting slow and fast leaks, high consumption, etc. The data accumulated within the portal is received from a cellular endpoint residing in the field.	10.00%	* Improved customer service with a detailed capture of usage such as spikes and interruptions that may identify leaks * Reduced truck-rolls to remote sites and infrastructure reduces costs and increases safety * Provide real-time and historical data analytics to improve operational efficiency and reduce related costs * The cloud-based application provides real-time insight into asset performance via any web-enabled device or handset decreasing response time to critical field failures * Highly flexible system allows low-cost and simple integration with existing systems * Non-proprietary hardware allows for quick availability and competitive costs on off-the shelf hardware across multiple OEM's * Future Proof- Designed and interoperable with systems added later * Resilient- cellular service is one of the first systems to be restored so once it is up and running the water meter data is flowing and repopulating readings captured during downtime
				10.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$150.00				

Configure

Configure

MA3696 Wireless Voice, Data and Accessories Attachment C: Costsheets					
Award Category 3-O Costsheets					
Vendor Name:				US Cellular	
	Product Name	Product Description	Characteristics of Product	Percentage Off Discount (%)*	Notes
	Connect Anywhere Monthly Service	The SkyHawk ConnectAnywhere web-based monitoring solution is an enterprise level, cloud based service which facilitates the real-time visibility and management of an organization's valuable assets. The service provides unique asset identification, GPS location and vehicle status integration with sensory information such as plow, spreader, PTO, beacon and brooms.	Four levels of service available: Professional, Express, Lite, and Asset. Providing the features and pricing to meet your business needs. Services are priced per asset, with an unlimited number of users, reports, and usage	15.00%	Connectivity/Data rates for required plans will be provided as per US Cellular rates & discounts submitted separately with the RFP
				15.00%	
*The Offeror with the highest proposed minimum discount % (or Average discount off) for the given subcategory will receive 100% of the cost points possible for that service category. All other Offerors will receive a percentage of the cost points possible based on the percentage by which their proposed discount % is lower than the highest discount % in the given category. The formula to compute cost points is: (Proposed Discount % / Maximum Proposed Discount %) * Total Cost Points Available.					
Consultative Hourly Rate (this rate will be included in the contract)	\$150.00				

Fill in each column for each plan or feature included. Enter "not applicable" or "N/A" for any column that does not apply to a specific plan or feature.

Name	Description	Pricing	
Chameleon CTM-200 LTE with USB Stick	Chameleon CTM-200 LTE with USB Stick (UML397)	\$	Cypress Chameleon CTM-200 LTE with USB Stick
Chameleon CTM-200 LTE with Chipset	Chameleon CTM-200 LTE with Chipset (MC7354v2)	\$ 714.00	Cypress Chameleon CTM-200 LTE with Chipset
Chameleon CTM-ONE CAT 1 includes ECM	Chameleon CTM-ONE 4G-Lte-Cat1 includes ECM	\$	Cypress Chameleon CTM-ONE CAT 1 includes ECM
CTM-200 Power Cable	CTM-200 Power Cable	\$ 15.95	Cypress CTM-200 Power Cable
CTM-200 IO Block	CTM-200 IO Block	\$	Cypress CTM-200 IO Block
CTM-200 ECM CAN Cable	CTM-200 ECM CAN-Cable	\$ 18.75	Cypress CTM-200 ECM CAN Cable
CTM-200 Y-Split CAN Cable	CTM-200 Y-Split CAN-Cable OBDII or J1939	\$ 18.75	Cypress CTM-200 Y-Split CAN Cable
Windshield Antenna	Windshield Antenna (GPS/Cellular)	\$	Cypress Windshield Antenna
Windshield Antenna Pad	Replacement Windshield Antenna Pad	\$	Cypress Windshield Antenna Pad
Wi-Fi Bluetooth Antenna	Wi-Fi / Bluetooth Antenna	\$ 16.00	Cypress Wi-Fi Bluetooth Antenna
GPS Only Mag-Mount Miniature	GPS Only Mag-Mount Miniature	\$	Cypress GPS Only Mag-Mount Miniature
LTE Dual Band Blade	Cellular Only LTE Dual Band Blade	\$ 11.25	Cypress LTE Dual Band Blade
Spreader Data Cable	Spreader Data Cable	\$ 12.50	Cypress Spreader Data Cable
Protective Case with Clear Lid	Protective Case with Clear Lid	\$	Cypress Protective Case with Clear Lid
Hydraulic Sensor 6 feet 4-wire lead	Hydraulic Sensor w/6 feet 4-wire lead	\$ 152.00	Cypress Hydraulic Sensor 6 feet 4-wire lead
Proximity Plow Sensor Kit	Proximity Plow Sensor kit w/ LED Cable & bracket	\$	Cypress Proximity Plow Sensor Kit

Ready Wireless CalAmp LMU 3030	CalAmp LMU 3030	OBDII LTE device. One-time fee.	\$158.00
Ready Wireless CalAmp LMU 2630	CalAmp LMU 2630	Hardwired LTE device. One-time fee.	\$122.00
Ready Wireless CalAmp LMU 2630	CalAmp LMU 2630	Kit Hardwired LTE device. Includes Power Harness. One-time fee.	\$132.00
Ready Wireless CalAmp LMU 4230	CalAmp LMU 4230	Hardwired LTE device with Bluetooth. One-time fee.	\$185.00
Ready Wireless CalAmp LMU 4230	CalAmp LMU 4230	Kit Hardwired LTE device. Includes Power Harness, JPOD and External Antenna. One-time fee.	\$307.00
Ready Wireless CalAmp LMU 3640	CalAmp LMU 3640	Hardwired LTE device with Bluetooth. One-time fee.	\$195.00
Ready Wireless Cal Amp LMU 3640 Kit	Cal Amp LMU 3640 Kit	Hardwired LTE device. Includes Power Harness and JPOD. One-time fee.	\$263.00
Ready Wireless OBDII Extender Cable	OBDII Extender Cable	Extender cable for OBDII port. One-time fee.	\$5.50
Ready Wireless Power Harness	Power Harness	For hardwired devices. One-time fee.	\$16.00
Ready Wireless JPOD	JPOD	JPOD Cable. Please specify Medium or Heavy. One-time fee.	\$53.00
Ready Wireless External Antenna	External Antenna	External Antenna mainly for devices with no internal antenna. One-time fee.	\$53.00
Ready Wireless Extender Cable	Extender Cable	Ready Fleet Extender Cable	\$5.30
Ready Wireless Y Cable	Y Cable	Ready Fleet Y Cable	\$10.70
Ready Wireless CalAmp TTU 2830	CalAmp TTU 2830	ReadyFleet - RF2830 LTE (US Cellular) - Trailer Tracker	\$160.00
Ready Wireless CalAmp TTU 2830 with Temp probe	CalAmp TTU 2830 with Temp probe	ReadyFleet - RF2830 LTE (US Cellular) - Refrigerator Trailer Tracker, 1 Temperature Probe	\$170.00
Ready Wireless CalAmp TTU 2830 with Starter Interrupt	CalAmp TTU 2830 with Starter Interrupt	ReadyFleet - RF2830 LTE (US Cellular) - High Value Asset Tracker (Starter Interrupt)	\$170.00
Ready Wireless Geometris 95 Series	Geometris 95 Series	Fleet Tracking device	\$80.00
Ready Wireless Geometris 96 Series	Geometris 96 Series	Fleet Tracking device. Bluetooth enabled	\$100.00

CalAmp LMU 3030	MiFleet - MF3030 LTE (US Cellular) - OBD Plug'n Play	####	MiFleet CalAmp LMU 3030
CalAmp LMU 2630	MiFleet - MF2630 LTE (US Cellular) - 3 Wire Installation, Power Cable, Internal Antenna & Backup Battery	\$110.00	MiFleet CalAmp LMU 2630
CalAmp LMU 4230	MiFleet - MF4230 LTE (US Cellular) - 3 Wire Installation, 5c888 Power Cable, Bluetooth, External Antenna Included	####	MiFleet CalAmp LMU 4230
CalAmp TTU 2830	MiFleet - MF2830 LTE (US Cellular) - Trailer Tracker	####	MiFleet CalAmp TTU 2830
CalAmp TTU 2830 with Temp Probe	MiFleet - MF2830 LTE (US Cellular) - Refrigerator Trailer Tracker, 1 Temperature Probe	####	MiFleet CalAmp TTU 2830 with Temp Probe
CalAmp TTU 2830 with Starter Interrupt	MiFleet - MF2830 LTE (US Cellular) - High Value Asset Tracker (Starter Interrupt)	####	MiFleet CalAmp TTU 2830 with Starter Interrupt
CalAmp LMU 3640	MiFleet - MF3640L-US - 3 wire installation, internal antenna, Bluetooth included	####	MiFleet CalAmp LMU 3640
Geometris 95 Series	LTE CAT-1 95. USCC series with customer applied SIM. OBDII/J1939 (auto-detection) & BLTE	\$85.00	MiFleet Geometris 95 Series
Geometris 96 Series	LTE CAT-1 85. USCC series with customer applied SIM. OBDII/J1939 (auto-detection) without BLTE	\$110.00	MiFleet Geometris 96 Series
9 Pin Square Connector	J1939 (9 Pin Deutsch) Square Connector, Y Harness for use with 8X series. 3ft length.	\$25.00	MiFleet 9 Pin Square Connector
9 Pin "D" Style Connector	J939 (9 Pin Deutsch) "D" Style Connector, Y Harness for use with 8x series. 3 ft length	\$22.00	MiFleet 9 Pin "D" Style Connector
6 Pin Connector	J1708 (6 Pin Deutsch) Y Harness for use with 8X series. 3 ft length	\$25.00	MiFleet 6 Pin Connector

Financial health of company

All offerors to this RFP must provide to the State a Dun and Bradstreet (D&B) number and report in their submission.

Offerors must meet at a minimum, Dun and Bradstreet rating of BB2 or better.

Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

If a government entity is bidding on this RFP, a D&B rating and number is not required for the government entity.

D&B rating may be provided by a D&B report, or any other verifiable means as an attachment to your proposal.

USCC Services, LLC (d/b/a UScellular) Dunn and Bradstreet Rating: 5A

DUNS: 11-823-9292

Please see the full Dunn and Bradstreet Report for additional information.

UNITED STATES CELLULAR CORPORATION

Tradestyle(s): (SUBSIDIARY OF TELEPHONE AND DATA

SYSTEMS, INC., CHICAGO, IL) +1

ACTIVE

HEADQUARTERS

Address: 8410 W Bryn Mawr Ave Ste 700, Chicago,
IL, 60631, UNITED STATES

Phone: (773) 399-8900

D-U-N-S: 11-823-9292

In Portfolio: No

D&B Rating

Current Rating as of 02-26-2016

Financial Strength

Risk Indicator

5A : US\$ 50,000,000
and over in Net
Worth or Equity

1 : Very Low Risk

MA3696 Attachment S

The State of Utah

Department of Administrative Services

Division of Purchasing and General Services

In conjunction with NASPO ValuePoint

Attachment S

Utah Solicitation # CJ21-3

Security Disclosure Statement

Utah Solicitation # CJ21-3



NASPO

ValuePoint



- A. Purchasing entities are concerned about the security and privacy of information and data related to the performance of this contract. The type of data and information transmitted, stored and processed by the products and services will vary based on the purchasing entities requirements. As a result, it is not possible to establish a single set of security requirements all products and services awarded under this contract must meet. Each purchasing entity purchasing from this contract will determine which products and services have the appropriate cyber security and data controls in place to meet their specific needs. To assist public entities each offeror must submit a Security Disclosure Statement with their proposal.

UScellular has complied. This document outlines the security in place for our network and for the vendors we partner with to deliver our services. Please see the attached UScellular Security Disclosure Statement Response – All Vendor Info spreadsheet for a detailed response from each of the vendors we partner with for these solutions.

- B. To qualify for any award under this contract, the Offeror must submit a Security Disclosure Statement addressing all of the elements listed below.
- i. In responding, Offeror must address not only the security mechanisms used by the bidder and its direct subsidiaries, but any partners, subcontractors or other 3rd parties who would be involved in implementing, operating, or in any way coming into contact with the service.
 - ii. By signature of the proposal submitted in response to this RFP, the offeror represents and warrants the accuracy and currency of the information submitted in response to the Security Disclosure Statement as listed in paragraph C of this attachment.

UScellular has complied.

- C. Security Disclosure Statement information required. Offeror shall describe all policies, procedures, measures, methods, certifications and standards the offered product and/or service has in place to protect the purchasing entities security and privacy of information and data involved in the performance of this contract for each numbered statement below. Description responses shall also include;
- i. If for the specific product or service offered, the numbered security statement is not appropriate because it does not as a matter of accepted security practice relate to the product or service offered, the offeror shall indicate in a statement that it is not applicable and briefly explain why.
 - ii. If the specific product or service offered does not comply with the numbered statement, the offer shall indicate, "does not comply".
1. Methods and measures taken to hold, protect, and dispose of data during and following completion of any contract services. Include how access to a Purchasing Entity's user accounts or data will not be allowed, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

UScellular Methods and Measures taken to Hold, Protect and Dispose of Data

UScellular requires the secure handling of Information. Information includes all data that is electronically generated, printed, filmed, typed, stored, handwritten, or verbally communicated.

Information must be protected in accordance with laws and regulations, industry standards, contractual requirements, and information security best practices. Information must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the manual or automated systems that transmit or collect it, or the methods by which it is distributed and disposed.

Per Company policy, UScellular employees may only access an account for a legitimate business purpose.

UScellular defines the types of Information and its various categories in the **Information Classification Policy (CONFIDENTIAL - ATTACHED)**.

UScellular follows an **Information Handling Policy (CONFIDENTIAL - ATTACHED)** which ensures that Information, whether in physical or electronic format, is protected during all phases of its lifecycle.

UScellular employs a **Business Records Retention and Disposal Policy (CONFIDENTIAL - ATTACHED)** which applies to all organizations of Telephone and Data Systems, Inc., including UScellular. This policy outlines requirements for the retention and disposal of Business Records across all Company functions.

UScellular adheres to a **Business Records Retention Schedule (CONFIDENTIAL - ATTACHED)** which reflects the retention requirements specific to each Business Record type. The intention of the Business Records Retention Schedule is to ensure that the Company retains its Business Records long enough to meet its business needs, as well as comply with industry standards and legal requirements as set forth in state and federal laws.

Please see our [Privacy Statement](#) should you like to learn more about our collection, use, and sharing of Personal Information.

UScellular is a RISK based organization, protecting customer data to the best of our capability. User accounts and customer data is protected diligently. Data in motion and data at rest is isolated and protected by perimeter defense mechanisms like firewalls, IPS/IDS devices, monitored by advanced log aggregation and correlation systems, and protected by encryption standards.

Public Safety Systems are guarded by DDoS mitigation solution, Perimeter Firewalls, and Intrusion Detection Systems. Within the solution itself, intensive log correlation and monitoring is enabled for suspicious behaviors and abnormal traffic. UScellular also segmented the Quality, Priority, and Preemption service to its own dedicated mobile core network. UScellular also offers dedicated VPN connections from customers to its own network to provide specific and segmented services.

The vendors that we choose to partner with have IT Security policies in place that limit what data each employee can access based on their access level and the information needed to do their job. Requests are logged and logs are reviewed regularly. Customer administrators can control which users have access to what transactional data. Our IBM MaaS360 vendor, that provide services outside of the US, has logic in place to keep cloud data in that region.

In addition to covering data access, vendor Security policies are also in place to cover protection of company devices, email security guidelines, password management, data transfer, social media policies, etc. In general, data disposal and destruction does occur per existing security policy of seven years by default or other term agreed to by contract.

2. Security measures to secure and protect the confidentiality of information and data that is obtained, created, stored, transmitted, processed or otherwise held or managed by the product or service during the performance of all work related to performance of this contract. Include all data confidentiality standards and practices that prevent the exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data.

UScellular diligently protects user accounts and customer data. Data in motion and data at rest is isolated and protected by perimeter defense mechanisms like firewalls, IPS/IDS devices, monitored by advanced log aggregation and correlation systems, and protected by encryption standards.

The vendors that we choose to partner with have IT Security policies in place that limit what data each employee can access based on their access level and the information needed to do their job. Requests are logged and logs are reviewed regularly. Access is severed immediately upon employee separation.

Our vendors have all taken measures to ensure that data is encrypted, including data at rest, with some maintaining their data on the Cloud with standard encryption. Other vendors we partner with, like CyberReef, don't store data that passes through their systems.

3. Data encryption methods and standards in place to encrypt data at rest and in transit. This includes but is not limited to, encryption standards employed to protect data in transit over either wired or wireless (e.g. cellular, Wi-Fi, or other), and how that might change over the life of the contract.

UScellular follows UScellular Encryption Standard, copy of which is available in Appendix A, and industry standards like 3GPP encryption standards like 33.501 for the 5G security standards. Encryption is a cornerstone to provide confidentiality and integrity to data in transit and data at rest.

Specific to Public Safety Systems, customer owned/used device communication back to UScellular network is encrypted in public domain and segmented within UScellular network. Also, Secure LAN Access service provides end to end encryption and dedicated VPN tunnel from client site to UScellular's defined service under the contract.

Our vendors use various methods of encrypting data. Crexendo uses disk level encryption. IBM MaaS360 and Ready Wireless utilize AES-256 bit encryption for all data that is stored or transmitted. LEC encrypts data in transit via TLS. StreamWIDE uses TETRIS security features. Goldie uses a standard 128 bit encryption of data. GPS Trackit uses Amazon Web Services. ParkNav's data is stored in Google Cloud with standard encryption. SkyHawk's ConnectAnywhere solution is built upon MongoDB Atlas "Database as a Service" (DBaaS), which provides encryption at rest. End users access the system through a standard web browser, secured via HTTPS / TLS1.2. Simplifi secures user data by encrypting to storage. Their administration panel provides secure access by using encryption over HTTPS. CyberReef uses AES with high bit keys along with SHA hashing at varying levels along with Symmetric and Asymmetric key methods.

4. Measures to protect Information about the cost, type, quantity and location of state communications facilities, system assets, plans, procedures, contract information, billing

information and other information identified as sensitive by the purchasing entity related to the performance of all work under this contract.

UScellular diligently protects user accounts and customer data. Data in motion and data at rest is isolated and protected by perimeter defense mechanisms like firewalls, IPS/IDS devices, monitored by advanced log aggregation and correlation systems, and protected by encryption standards.

The vendors that we choose to partner with have IT Security policies in place that limit what data each employee can access based on their access level and the information needed to do their job. All such information is protected via encryption and selective access. No such data is available to the public or shared publicly or available online in any format.

Customer administrators can control which users have access to what transactional data. Our IBM MaaS360 vendor, that provides services outside of the US, has logic in place to keep cloud data in that region.

5. Risk and policy management and enforcement measures in place to protect the security of physical assets and information.

UScellular and our vendors have locations and access to physical infrastructure that is limited to authorized individuals. We have redundant Data Centers and disaster recovery plans in place that have been reviewed and tested.

Our vendors have similar physical security, redundancy and recovery plans in place, as well as Security Policy guides instructing employees how to respond to security incidents.

6. How distributed access is controlled and managed across IT assets, including data, applications, networks and platforms within the solution.

UScellular takes pride in its comprehensive Identity and Access Management Program. IAM program manages all wireless telecommunication as well as all internal authentication, authorization, and accounting needs. Comprehensive solution and management, as per our standards, provides support to external vendor and customer integrations in all current and available industry standard technologies like OAuth, OpenID, OIDC, SAML.

The vendors we partner with limit access to the least amount required for their employees to do their jobs. Many utilize Master Administrators to create custom roles with custom access rights. All access (user and administrative) is protected by multiple layers of secure accounts and encryption and are logged. In some cases, access is controlled through a CRM or restricted to the account owner through a set of known IPs (ParkNav). SkyHawk's ConnectAnywhere server infrastructure is hosted by Amazon Web Services (AWS) within a secure Virtual Private Cloud. This infrastructure is isolated from the public Internet, with access restricted through network and application load balancers; no services are directly accessible via the public Internet. CyberReef uses IP based ACLs to whitelist access to devices.

7. Security management in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center. ^(U)_(S)

UScellular Security organization is well established and situated to provide Confidentiality, Integrity, and Availability to its customers. UScellular employs magnitude of services and processes to protect its network and customers.

Specific to Public Safety Systems and Secure LAN Access, as described in Question response 1, we have extensive security measures to protect customer communication and data from internal and external threats. If required, we would be more than happy to cover it in a scheduled meeting.

The vendors that we partner with limit access to their data centers both physically and logically to the minimum necessary for operations. Antivirus programs are in place to ensure detection, removal and alerting of malicious or unauthorized software. Networking principles are followed to protect against external threats. Patches and updates are maintained on computers, servers and operating systems on a regular basis.

8. Describe the logging process including:
 - a. The types of services and devices logged,
 - b. The event types logged, and
 - c. The information fields will be made available to the authorized Purchasing Entity if requested in their PA after award of the master agreement.

UScellular has a large log aggregation and correlation platform. UScellular processes over 50 Billion log events a day separated over 15 thousand log type with over 600 event type. Running over 500 correlations a minute. Increasing anomaly algorithms and detection algorithms provides visibility into all aspects of UScellular's network and processes. UScellular's logging policies and standards mandate that every device within UScellular forwards its logs to log aggregation layer.

Our vendors log a variety of activities including physical and logical access, logins, actions and events against devices, and significant data that is available to support personnel for debugging and identifying and troubleshooting system problems. Logging may also include access to and through servers, firewalls and applications as well as edge devices. Logging would generally include the user that accessed the data, the data being logged and the date/time in which it occurred.

9. Describe the security Technical Reference Architectures

We would be more than happy to discuss and display UScellular's proprietary Intellectual Property Technical Security Architecture as proper contractual agreements put in place.

It is difficult to summarize the details from our vendors. However, here is some additional information.

IBM MaaS360 architecture documents can be found here:

https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/references/ce_architecture.htm

CyberReef partners with Lumen and they have a variety of physical security measures ranging from fingerprints to optical scanners. All gear is kept in secure cages. All data is transient with nothing retained.

Crexendo data center deployment consists of one or more layers of network address translation (NAT) and firewalls to regulate the access to deployed applications. Individual applications authenticate users over secure transport before allowing access to data the users are privileged to access.

Please see the UScellular Security Disclosure Statement Response – All Vendor Info spreadsheet for more details on vendor solutions.

10. Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offerors employees who have access to sensitive data.

Locations, details, and access to physical infrastructure is limited to authorized individuals on a need-to-know basis. UScellular employees undergo a background check and drug screening prior to hire. Our vendors have similar restrictions and policies in place.

11. Provide an itemized list of all cyber security standards and, security certifications in place that the products and service offered comply with to ensure appropriate controls and data confidentiality are in place, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800- 171, FIPS 200 and FedRAMP (Moderate, High) if they apply. Include detailed response on how security standards and certifications will be maintained and updated to meet best practices for maintenance and operations.

Please see attached UScellular Security Disclosure Statement Response – All Vendor Info Spreadsheet for details

12. Provide a detailed list of all third-party attestations, security credentials and certifications, and reports relating to data security, integrity, and other controls in place.

UScellular is a respected organization in the industry, who partners with industry leading third-party service providers for their products and services. UScellular has high standards on vendor management and accountability requirements that it holds its vendors to. Upon proper NDA and contractual agreements, UScellular vendor management team can share more appropriate information.

Please see attached UScellular Security Disclosure Statement Response – All Vendor Info Spreadsheet for vendor details.

13. NIST Cybersecurity Framework, April 16, 2018,Version 1.1
<https://doi.org/10.6028/NIST.CSWP.04162018>: Describe how the offeror is prepared to utilize the NIST Cybersecurity Framework for Turnkey Internet of Things, Other Turnkey Wireless, Applications and Services (Category 3) and Wireless Transport Options (Category 4) as may be implemented by the Purchasing Entity, which may include, but is not limited to:
 - a. Convey the purchasing entities' cyber security requirements,

- b. Identify Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities will provide in the Offerors's system, products or services under contract with the Purchasing Entity,
- c. Communicate cyber security requirements through Cyber Supply Chain Risk Management (SCRM), and
- d. Other cybersecurity risk management activities of Offeror's system, products or services under contract with the purchasing entity.

NIST Cybersecurity Framework is developed in response to Executive Order issued in February 2013; framework released February 2014. Latest version is released in April 16, 2018. NIST CSF is a living and breathing framework that it constantly evolves and improves itself. UScellular adopted NIST early 2016 and has been utilizing the framework and adopting the changes as they are released. UScellular goes through yearly self-assessments to find improvement points and defines projects to move the ball forward every year. UScellular also welcomes external assessment every 3 years to validate its self-assessments and how it is tracking the program. Upon proper NDA and contractual agreements, we can walk through our environments current state relevant to NIST controls.

Please see attached UScellular Security Disclosure Statement Response – All Vendor Info Spreadsheet for information on how our vendor partners comply to this standard.

- 14. NIST Cybersecurity Framework, Table 2 Framework Core: For each subcategory of the all 15 Categories of the NIST Cybersecurity Framework, list the specific standards and certifications, the products or services offered comply with at the time of your proposal. Categories Include:
 - a. Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Security – UScellular Confirms

UScellular has implemented asset management systems

- b. Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Security – UScellular Confirms

- c. Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Security – UScellular Confirms

UScellular has implemented detailed governance policies and procedures.

- d. Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Security – UScellular Confirms

UScellular has implemented risk assessment policies and procedures

- e. Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

UScellular has implemented a risk management strategy with documented policies and procedures

- f. Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Security - UScellular confirms

- g. Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Security – UScellular Confirms

UScellular has implemented comprehensive identity management, authentication, and access control systems, policies, and procedures.

- h. Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

UScellular confirms.

The Company's Privacy Policy sets the expectation that all Associates take the required training for Privacy and Information Security as outlined below and that Leaders ensure that their Associates take the required training. All Associates are required to comply with the Privacy Policy as stated in the Company's Code of Business Conduct.

- i. Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Security - U.S. Cellular confirms.

U.S. Cellular has implemented policies and procedures for data security including standards for encryption, integrity checking, data loss prevention, etc.

- j. Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Security - U.S. Cellular confirms.

U.S. Cellular has implemented information protection policies, processes and procedures.

- k. Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Security - U.S. Cellular confirms.

- l. Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Security - U.S. Cellular confirms.

- m. Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.

Security - U.S. Cellular confirms.

- n. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Security - U.S. Cellular confirms.

- o. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

Security - U.S. Cellular confirms.

- p. Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Security - U.S. Cellular confirms.

- q. Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

Security - U.S. Cellular confirms.

- r. Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.

Security - U.S. Cellular confirms.

- s. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

Security - U.S. Cellular confirms.

- t. Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Security - U.S. Cellular confirms.

- u. Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

Security - U.S. Cellular confirms.

- v. Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.

Security - U.S. Cellular confirms.

- w. Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

NIST Cybersecurity Framework is developed in response to Executive Order issued in February 2013; framework released February 2014. Latest version is released in April 16, 2018. NIST CSF is a living and breathing framework that it constantly evolves and improves itself. U.S. Cellular adopted NIST early 2016 and has been utilizing the framework and adopting the changes as they are released. U.S. Cellular goes through yearly self-assessments to find improvement points and defines projects to move the ball forward every year. U.S. Cellular also welcomes external assessment every 3 years to validate its self-assessments and how it is tracking the program. Upon proper NDA and contractual agreements, we can walk through our environments current state relevant to NIST controls.

Please see attached U.S. Cellular Security Disclosure Statement Response – All Vendor Info Spreadsheet for information on how our vendor partners comply to this standard.

15. Describe the data breach/incident policies and procedures regarding notification to both the purchasing entity of a security incident and/or data breach, as defined in this RFP, and the mitigation of such a breach. Include how proposer will work with Purchasing Entities before, during, and after a Security Incident and a Data Breach. Include information such as:
- Personnel who will be involved at various stages, include detail on how the Contract Manager will be involved;
 - Response times;
 - Incident levels;
 - Processes and timelines; ^[11]_[SEP]
 - Methods of communication and assistance; and
 - Other information vital to understanding the service you provide. ^[11]_[SEP]

Provider should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Personnel

Once a data security event ('Event') has been reported to the UScellular Incident Management team, the UScellular Incident Management team engages the UScellular Data Security Event Response Team ('DSERT').

The DSERT investigates and analyzes the Event to determine whether it is an Incident.

Upon the decision that an Incident has occurred, the UScellular Extended Data Security Event Response Team ('EDSIRT') is engaged to work with the DSERT and develop the Company's organizational response.

Timelines

Timelines are variable.

Process

UScellular's organizational response to an Incident is as follows: Containment, Eradication, and Recovery.

- **Containment** of the Incident must be completed before progressing to Eradication and Recovery. Absent Containment, the Incident can overwhelm resources and continue to cause corruption. Containment strategies vary.
- **Eradication** may be necessary to eliminate components of the Incident, such as deleting malware and disabling breached user accounts. Eradication also is used to identify and mitigate the vulnerabilities that were exploited.
- In **Recovery**, administrators restore systems to normal operations, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar Incidents.

UScellular Security Organization takes the security threats seriously. UScellular employs incident response procedures to respond to all security incidents within a timely fashion.

When a security incident is reported and an incident handler from the Incident Management team has been assigned. Incident response teams are composed of IS and Engineering resources as deemed appropriate to the incident. Team members must respond to and resolve all incidents reported by the Incident Management team.

All our vendors have methods for dealing with security incidents in a timely fashion, ensuring that the right individuals are involved to resolve the problem as quickly as possible and provide notification and updates. Please see attached UScellular Security Disclosure Statement Response – All Vendor Info Spreadsheet for more details on how each of our vendors handle these incidents.

16. Describe the method for compliance with all applicable laws related to data privacy and security including state Security Breach Notification Laws dealing with personally identifiable information (PII). Describe any legal obligations related to security the offeror will meet over the life of the contract and describe how offeror will report changes to these obligations to the public entity.

UScellular observes applicable laws related to data privacy and security including state Security Breach Notification Laws dealing with personally identifiable information (PII).

Our vendors would be required to observe applicable laws and have provided details on how they would do that via the attached UScellular Security Disclosure Statement Response – All Vendor Info Spreadsheet.

- D. Any Turnkey Internet of Things, Other Turnkey Wireless system that incorporates SaaS, IaaS or PaaS or other cloud computing element shall complete, provide, and maintain a completed CSA STAR Registry Self-Assessment for that element. 2 < https://cloudsecurityalliance.org/star/self-assessment/#_overview . Offeror must either submit a completed Consensus Assessments Initiative Questionnaire (CAIQ), or submit a report documenting compliance with Cloud Controls Matrix (CCM) that the CAIQ is based on for the element that cloud based.

It is our intent to gather this information from our vendor partners and to provide it to you using either of the two options requested. Further details on which of the two options will be selected can be reviewed during follow-up discussions or at the time of contract negotiations.

MA3696 Combined Attachments Q and T

Appendix B

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory A: Fleet Management

GPS Trackit



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
GPS Trackit Fleet Manager
- b. General Application Area
Subcategory A: Fleet Management
- c. General capabilities provided
Provide real-time vehicle-based GPS tracking and management system including device to be either hardwired under or Plug and Play (PnP) into the OBDII port.
- d. Expected impact on cost/performance/functionality, etc.
The efficiencies gained in maintenance behavior, vehicle performance, reducing idle time, improving fuel consumption, and route guidance are significant. The ability to score and manage distracted driving behavior and greatly reduce risk is immeasurable.
- e. Subcontractors/partners involved in delivering service
UScellular partners with GPS Trackit and Geometris to provide this solution.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes. See attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
Since 2002, GPS Trackit has been a pioneering force in cloud based, IoT fleet solutions and GPS fleet tracking. Benefits of Cloud-Based GPS Tracking Software include:
 - Save Money- With our fleet management solutions, you can monitor and streamline labor costs.
 - Save Time- GPS Trackit's solutions help you streamline tasks and boost productivity.
 - Track & Protect Assets- By monitoring driver behavior, our customers have seen accident risks fall by one-third.
 - Monitor Real-Time Data- Monitoring and identifying driver behaviors can reduce fuel waste.
 - Experience Expert Support- Our customer service experts are here to help your business every step of the way.
- b. Applicability to government needs
Detailed interactive maps, robust reporting, customized automation as well as asset and vehicle theft protection are benefits that would serve government needs well.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references

Our industry-leading technology and focus on world-class customer service has earned us a place on Deloitte's Technology Fast 500 list and supports over 12,000 fleets worldwide.

Reference	
Name of Entity	City of Strongsville
Service Provided	Fleet Management Solutions
Years in Use	7
Number of Vehicles	30+
Date of Provision	01/15/2013
Address:	13213 Pearl Rd. Strongsville OH. 44136
Contact	Katie Grace
Telephone	440-238-9936
Email	katie.grace@strongsville.org

Reference	
Name of Entity	Mica Corporation
Service Provided	Fleet Management Solutions
Years in Use	8
Entity Size & Scope	277 Vehicles
Date of Provision	1/12/2012
Address:	9 Mountain View Drive Shelton, CT 06484
Contact	Raun Deosarran
Telephone	817-847-6121 x220
Email	raun@micacorporation.com

Reference	
Name of Entity	Arizona Pipeline
Service Provided	Fleet Management Solutions
Years in Use	6
Entity Size & Scope	800 Vehicles
Date of Provision	12/12/2014
Address:	17373 Lilac St Hesperia, Ca
Contact	Neil Christensen
Telephone	760-559-4281
Email	nchristensen@arizonapipeline.com

- d. Overall interoperability of turnkey system for government use
Ease of use, multiple user capability, and unlimited training are all benefits of this turnkey system that would benefit government users.
- e. Accessories available for turnkey offering
Our turnkey system comes ready to use. The only accessory potentially needed would be a relocation cable.
- f. Thoroughness of the vetting process used to select partners
Our hardware, software and associated tools are fully compliant with the Association of Equipment Management Professionals (AEMP) standards, which are also now approved by the International Standards Organization (ISO 15143-3:2016).
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
Data is one of your company's most important assets. We ensure our end-to-end solutions protect the data that drives your business.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package. The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
We have an onboarding team that will coordinate with the point of contact with the state or municipality.

b. Project coordination

We at GPS Trackit pride ourselves in our seamless process for the implementation of our solution that will allow you to onboard without stress or delay. GPS Trackit differentiates its implementation and customer onboarding process from its competitors by working very closely with you to establish a specific timeline for complete deployment as suited to your needs and will support you throughout the transition process. Upon completion of the sale, GPS Trackit will process your order in 5-7 business days (standard order processing time). We will ship the products to you at the earliest possible time using a third-party carrier. Shipping turnaround time is typically between 24 and 48 hours (business days). GPS Trackit units are designed to be conveniently self-installed. Many of our clients prefer to have their units installed by professionals to ensure that the installation has been performed correctly. If you prefer to have your units professionally installed, we will access our extensive network of subcontractors and identify a local installer who we are confident can perform the installation to your satisfaction.

We will work with you to set up a date for your first software training at your earliest convenience, which will help you understand how to get the most out of your new GPS Trackit products. We are willing to work with you until you're completely satisfied with your purchase. Your personalized training plan will be designed around your needs and the user groups who will be receiving the training.

c. Installation and Testing process

Our dedicated support team will work to facilitate the activation and testing of all devices.

d. Client Infrastructure and support assessment process

The proposed software is based upon a 3-tiered, browser-based architecture and the core software was written in 2007. The proposed solution does not require any software other than a browser to be installed on the client workstation. There is no add-on or third-party software required to support the functionality desired by the state or municipality. The programming languages used for development and configuration of the proposed solution are Ruby, C# and Java. Web application, mobile, data processing and gateways are proprietary components of the software. The solution is dependent on open source software.

e. End user Acceptance process

User acceptance is an online process for our customers.

f. Approach to maintenance and support

Please refer to h.

g. Initial and Ongoing Training provided

Unlike other GPS tracking companies, we provide you with unlimited free live training anytime you need it. That means if you have new employees or just want a refresher course, it's available. We never limit the length of training or cap the number of times you can receive it. For your convenience, we offer both group and one-on-one trainings.

h. On-going support and enhancement over the life of the agreement

GPS Trackit has an extensive resource of online training and support materials available for clients through <http://support.GPSTrackit.com/>. We are also available to provide any required support, technical as well as otherwise, our dedicated support teams are available at all times to assist you.

All of our clients are always hosted on the latest version of software. Typical software maintenance and updates to the software are pushed to all clients without interruption. Upgrades under the original scope of services are included at no additional costs. Any upgrades mandated by GPS Trackit will be at our cost. Our engineers are constantly working on both, proactive as well as reactive maintenance procedures to ensure that the software is performing at optimal levels.

1st-Tier Support is provided by experienced product specialists. If a case requires additional support, it will be escalated within 24 hours to the appropriate department. Account Managers will also be available to track and manage the support case and resolution process.

4 - Service Factors:

a. Description of related services included in Turnkey Solution

Service plan features include:

- Update Frequency: 1 Minute Updates (also capable of 30 second updates)
- Detailed Reporting, Scheduled Automatic Email Reports: Activity Summary, Clock In/Out, Engine Run Time, Idle Time, Ignition Events, Landmark Events, Latitude & Longitude, Mileage, Speed Sample, State Mileage, Stops
- Mapping Views: Satellite Imaging, Street View, and Hybrid View powered by Google Maps
- Create and Manage: Geofences, Landmarks, Contacts, Drivers, Vehicles, and Routes
- Software Management Tools: User-Based Permissions & Access Restriction, Unlimited Sub-User Creation, Unlimited Access to Historical Data
- Find and Generate Turn-by-Turn Directions to Equipment, Landmark, or Nearest Vehicle
- Driver Behavior Monitoring & Alerts: Landmark In/Out, Exceeding Posted Speed Limit, Hard Braking, Hard Turning, Rapid Acceleration
- Customizable Alerts: Off-Hours Activity/Unauthorized Use, Power or Antenna Disconnect, Service Required (according to Miles, Days, or Engine Hours), Landmark Entered/Exited
- Vehicle Views: Vehicle Trails/Movement Histories, Trip Comparisons, Geofences, Landmarks, Driver Events
- Traffic Information
- Track and Manage Equipment
- Power Take-Off Event Monitoring

b. Experience and qualifications of partners and subcontractors

20 plus years in business

c. Description of Additional Integration and Consulting Services provided

N/A

END USER LICENSE AGREEMENT

This End User License Agreement (this “EULA”) governs your use of the software and related services (the “Software”) of Global Tracking Communications, LLC (the “Company”), for use pursuant to and subject to certain terms and conditions between the Company and your employer (“Licensee”). All users of the Software are subject to the terms and conditions contained in this EULA.

BY CLICKING THE “ACCEPT” BUTTON OR CHECKING THE “ACCEPT” BOX YOU: (i) REPRESENT THAT YOU ARE DULY AUTHORIZED BY LICENSEE TO ACCESS AND USE THE SOFTWARE; AND (ii) ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS EULA AND AGREE THAT YOU ARE LEGALLY BOUND BY THEM. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS EULA, DO NOT CLICK THE “ACCEPT” BUTTON OR CHECK THE “ACCEPT” BOX AND YOU WILL HAVE NO LICENSE TO, AND MUST NOT ACCESS OR USE, THE SOFTWARE.

1. LICENSE GRANT TO USE THE SOFTWARE

Subject to your strict compliance with this EULA, the Company hereby grants you a non-transferable, non-exclusive, non-sublicensable, limited license to use the Software solely for business purposes on behalf of Licensee. You do not receive title to the Software and you may not distribute or use the Software other than for the purposes set forth in this EULA. You may not modify, adapt, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software. You may not create any derivative works of the Software. The Software is subject to all restrictions on use, disclaimers of warranties and other provisions in this EULA. The Company reserves all rights not expressly granted to you.

2. TERMINATION OR RESTRICTION OF ACCESS

Your license to use the Software is effective until terminated. You may terminate the license at any time by uninstalling the Software and deleting any related data from your device(s).

This EULA and your right to use the Software will terminate immediately without notice if you fail to comply with this EULA. The Company may terminate or suspend your access to the Software at any time. Upon termination, you agree to immediately cease using and to uninstall the Software from your devices(s), including all accompanying documentation and materials.

3. PROPRIETARY INFORMATION

The entire contents of the Software (including all information, text, displays, images, video and audio and any software made available through or in connection with the Software) and the design, selection and arrangement thereof, are proprietary to the Company or its affiliates or licensors and are protected by United States and international laws regarding copyrights, trademarks, trade secrets and other proprietary rights. You are only authorized to use the content on the Software for business use on behalf of Licensee. You may not copy, modify, create derivative works of, publicly display or perform, republish, store, transmit or distribute any of the material of the Software without the prior written consent of the Company. Neither the title nor any intellectual property rights to any material in the Software are transferred to you, but instead will remain with the Company or the applicable owner of such content. Except as expressly authorized by the Company in writing, you may not reproduce, sublicense, distribute, sell or exploit for any commercial purposes any part of, or access to, the Software.

The Company name and logos, and all related names, logos, product and service names, designs and slogans contained in the Software are trademarks of the Company, its affiliates, licensors and/or contractors unless otherwise clearly specified in writing. You may not use such marks without the prior written permission of the Company. All other names, brands and marks are used for identification purposes only and may be the trademarks of their respective owners. All rights are reserved.

4. COLLECTION AND USE OF INFORMATION

The Company may, directly or indirectly through the services of others, collect and store information regarding use of the Software and about equipment on which the Software is installed or through which it otherwise is accessed and used, by means of providing maintenance and support services.

You agree that the Company may use such information for any purpose related to any use of the Software by you, including but not limited to: (i) improving the performance of the Software or developing updates; and (ii) verifying compliance with the terms of this EULA and enforcing the Company's rights, including all intellectual property rights in and to the Software.

5. DISCLAIMER OF WARRANTIES

THE COMPANY, ITS AFFILIATES AND ITS LICENSORS EXPRESSLY DISCLAIM ANY AND ALL REPRESENTATIONS AND WARRANTIES (EXPRESS OR IMPLIED) IN CONNECTION WITH THE USE AND OPERATION OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, EFFECTIVENESS, COMPLETENESS, ACCURACY, TITLE, AND NONINFRINGEMENT, OR ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE. NONE OF THE COMPANY, ITS AFFILIATES OR ITS LICENSORS WARRANTS THAT THE SOFTWARE IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS.

THE FOREGOING PROVISIONS SET FORTH IN THIS SECTION ARE ESSENTIAL PARTS OF AND CANNOT BE SEVERED FROM THIS EULA.

6. LIMITATION OF LIABILITY

YOU WAIVE THE ABILITY TO ASSERT A CLAIM AGAINST THE COMPANY MORE THAN ONE (1) YEAR AFTER THE FIRST EVENT OR FACT THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL THE COMPANY, ITS AFFILIATES OR ITS LICENSORS BE HELD LIABLE TO YOU OR ANY OTHER PARTY FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS OR BUSINESS OPPORTUNITIES), REGARDLESS OF THE LEGAL THEORY, WHETHER SUCH DAMAGES WERE FORESEEABLE, OR WHETHER THE COMPANY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE COMPANY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THIS EULA EXCEED \$100. THESE LIMITATIONS OF LIABILITY SHALL SURVIVE THE TERMINATION OF THIS EULA.

THE FOREGOING PROVISIONS SET FORTH IN THIS SECTION ARE ESSENTIAL PARTS OF AND CANNOT BE SEVERED FROM THIS EULA.

7. INDEMNIFICATION

You agree to indemnify and hold harmless the Company and its shareholders, partners, affiliates, directors, officers, subsidiaries, employees, agents, suppliers, third party information providers, licensors,

licensees, distributors, contractors and others involved in providing the Software and related online services (collectively, the “Indemnified Parties”), from and against any and all liabilities, expenses, damages and costs, including reasonable attorney’s fees, arising from any violation by you of this EULA.

The foregoing provisions set forth in this Section are essential parts of and cannot be severed from this EULA.

8. COMMENTS AND SUBMISSIONS

The Company welcomes your comments with respect to the Software. All comments, suggestions or other information sent by you to the Company will become the Company’s property. For avoidance of doubt, the Company shall own any developments by the Company or on its behalf arising out of your comments, suggestions or other submissions. To the extent the Company does not own such materials, you grant and agree to grant the Company a perpetual, irrevocable, non-exclusive, royalty-free license to utilize, create derivative works of, distribute and sublicense such materials for any purpose in connection with the Company’s web sites, products and services. You understand that all information you submit is non-confidential for all purposes, and you have no expectation of any review, compensation or consideration of any type for all submissions hereunder.

9. ARBITRATION

Any controversy or claim, whether based in contract, tort, statute, regulation or otherwise, between you and the Company or the Company’s subsidiaries or affiliates, and any of the Company’s officers, directors and employees, arising out of or relating to this EULA or your use of the Software, shall be adjudicated by binding arbitration, before a single arbitrator, in accordance with the Comprehensive Arbitration Rules & Procedures of JAMS (or any successor of that organization in effect at the time the arbitration is initiated) which shall administer the arbitration.

If you decide to initiate arbitration, the Company agrees to pay the filing fee required by JAMS to initiate your arbitration (up to \$250.00), and that the other costs of the arbitration proceeding will be split equally between you and the Company. You may hire an attorney to represent you. Each party to the arbitration shall bear its own costs and expenses related to such arbitration, regardless of which party prevails, but a party may recover any or all of its costs and expenses from the other party to the same extent as in court. The arbitration award shall be in writing and shall include findings of fact and conclusions of law. Judgment on the arbitration award may be entered by any court of competent jurisdiction. Either party may seek any interim or preliminary relief from a court of competent jurisdiction necessary to protect the rights or property of either party pending the completion of arbitration. You hereby agree that the arbitration will be held at the JAMS office closest to the Company’s principal place of business, Wilmington, Delaware, or any other location where you and the Company agree to hold the arbitration.

This section is deemed to be a written agreement to arbitrate pursuant to the Federal Arbitration Act (“FAA”), 9 U.S.C. §§ 1-16. You and the Company agree that this section is intended to satisfy the writing requirement of the FAA. The FAA will apply even though this EULA provides that it is governed by the law of the State of Delaware. **YOU HEREBY WAIVE THE RIGHT TO GO TO COURT, INCLUDING THE RIGHT TO A JURY. DISCOVERY AND RIGHTS TO APPEAL IN ARBITRATION ARE GENERALLY MORE LIMITED THAN IN A LAWSUIT AND OTHER RIGHTS THAT YOU WOULD OTHERWISE HAVE IN COURT MAY NOT BE AVAILABLE IN ARBITRATION.** You hereby acknowledge that you have read and understood the implications of this provision.

10. CHOICE OF LAW, VENUE.

This EULA and all questions of interpretation, construction and enforcement hereof, and all controversies arising hereunder, shall be governed by and construed in accordance with the applicable laws of the State of Delaware without giving effect to any choice or conflict of law provision or rule (whether of the State of Delaware or any other jurisdiction) that would cause the application of laws of any jurisdiction other than those of the State of Delaware. The state and federal courts in Wilmington, Delaware shall serve as the exclusive jurisdiction for any and all claims for interim or preliminary relief, as well as to enforce the confidentiality of arbitration, as set forth herein, and you hereby irrevocably and unconditionally waive any objection to the laying of venue of any action, suit or proceeding arising out of or in any way related to this EULA, in the state and federal courts located in Wilmington, Delaware, and hereby further irrevocably and unconditionally waive your right and agree not to plead or claim in any such court that any such action, suit or proceeding brought in any such court has been brought in an inconvenient forum.

The foregoing provisions set forth in this Section are essential parts of and cannot be severed from this EULA.

11. MISCELLANEOUS

Your use of the Software is subject to the Company's Privacy Policy, a current version of which is available here: <https://gpstrackit.com/privacy-policy/>.

You agree and certify that neither the Software nor any other technical data received from the Company, nor the direct product thereof (whether a process or service or otherwise), will be directly or indirectly exported or transmitted outside the United States except as authorized and as permitted by the laws and regulations of the United States. If the Software has been rightfully obtained by you outside of the United States, you agree that you will not re-export or transmit, directly or indirectly, the Software nor any other technical data received from the Company, except as authorized by the laws and regulations of the United States and the laws and regulations of the jurisdiction in which you obtained the Software. You agree that you will not export in any manner the Software without first obtaining all necessary approvals from the appropriate agencies in the United States and any other applicable countries.

The Software is a "Commercial Item" consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation" as such terms are defined in the Federal Acquisition Regulations ("FAR") at 48 CFR 2.101, developed exclusively with private funds. Consistent with 48 CFR 12.212, and the comparable DFAR in the DoD FAR Supp. at 227.7202-1 through 227.7202-4, the Software is licensed to you only as commercial software and only with the rights and obligations granted to public users generally as set forth above in the license grant contained in this EULA. Notwithstanding any other FAR, DFAR or other contractual provision into which this license agreement may be incorporated, any government end user only acquires the rights to use the Software as set forth in this EULA. The Software is acquired under the specific terms and conditions set forth herein. If any portion of the Software is deemed "non-commercial," or the following FARs or DFARs are deemed to apply, the Software is licensed under the terms hereof and under the RESTRICTED RIGHTS set forth in 48 CFR 52.227-19 and DFAR 252.227-7014 (and the government's use, duplication and disclosure rights are restricted as set forth therein).

Except as expressly set forth above, this EULA completely and exclusively states the agreement between you and the Company with respect to the Software, and no other terms that may have been communicated to you orally or in any other manner shall have any force or effect.

The Company's licensors and contractors are express third party beneficiaries of any of this EULA that are applicable to their products or services, including disclaimers of warranty and limitations of liability, and shall have the right to enforce directly against you all of your applicable representations, warranties, covenants, indemnifications and obligations under this EULA.

The Company's failure to insist upon or enforce strict performance of any provision of this EULA shall not constitute a waiver of the provision. Neither a course of dealing or conduct between you and the Company nor any trade practices shall be deemed to modify this EULA.

You agree that no joint venture, partnership, employment, or agency relationship exists between you and the Company as a result of this EULA or use of the Software.

A printed version of this EULA and of any notice given in electronic form shall be admissible in judicial or administrative proceedings based upon or relating to this EULA to the same extent and subject to the same conditions as other business documents and records originally generated and maintained in printed form.

Appendix C

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory A: Fleet Management

MiFleet



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
MiFleet
- b. General Application Area
Subcategory A: Fleet Management
- c. General capabilities provided
Fleet and Asset management solutions including, OBDII plug and play, Three wire covert solution, IP6X rated solutions for heavy duty equipment, and ELD solutions.
- d. Expected impact on cost/performance/functionality, etc.
 - Fairly priced
 - High performance
 - Top quality
 - Advanced functionality
- e. Subcontractors/partners involved in delivering service
UScellular partners with MiFleet and DCS to provide this solution.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
No.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
Devices manufactured by Calamp are considered to be best of breed telematics devices. Calamp telematics devices are used with some of the largest telematics applications in the United States. Devices cover the full OBD stack, providing the fleet manager with all OBD data (vehicle dependent).
- b. Applicability to government needs
We are not GSA certified.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
350 currently in successful use.

References:
Brunswick County
Duplin County

- d. Overall interoperability of turnkey system for government use
OBD devices are designed for all light duty (cars, vans, pick-ups) vehicles manufactured after 1998. Our OBD solution will work in any light duty vehicle and will report back (vehicle dependent) all OBD data from the vehicle. The OBD device can be easily removed from one vehicle and installed in another. Our additional offerings are wired solutions and must be wired into an asset or vehicle.
- e. Accessories available for turnkey offering
 - Starter interrupt
 - Panic button
 - Temperature monitoring probes
 - Power take off (PTO)
 - All six and nine pin cables needed for big rig trucks.
- f. Thoroughness of the vetting process used to select partners
Onboarding process followed.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
The solutions have been thoroughly tested prior to deployment. Our LTE solutions have been in the market for nearly two years.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
 - VIN numbers collected
 - VIN numbers per office / site / location
 - Coordinate with installer all installation information.
- b. Project coordination
A project manager is assigned.
- c. Installation and Testing process
Coordinated.
- d. Client Infrastructure and support assessment process
We have a clean SLA with all details.
- e. End user Acceptance process
Pilot testing.
- f. Approach to maintenance and support
All upgrades are done over the air (OTA) and we have a technical support team to assist.
- g. Initial and Ongoing Training provided
Training is ongoing with a web-based library containing all information needed for support.

- h. On-going support and enhancement over the life of the agreement
Yes.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
Assigned a project manager throughout the life of the project. High level of customer service.
- b. Experience and qualifications of partners and subcontractors
We have been selling our MiFleet solution for nearly five years.
The platform has more than 2.5M active subscribers. The solution is very scalable.
- c. Description of Additional Integration and Consulting Services provided
Throughout the life of the project.

Appendix D

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory A: Fleet Management

READY FLEET



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
READY FLEET powered by US Cellular Business
- b. General Application Area
Subcategory A: Fleet Management
- c. General capabilities provided
READY FLEET allows for any fleet manager to operate and track their vehicles efficiently with minimal equipment and maintenance. The intuitive platform allows for detailed reporting and insight to the 3 main "pillars" of fleet management: location/geotracking, maintenance/diagnostics and driver behavior. Unique to the platform is the ability to tether a driver's phone to the vehicle via the cloud and monitor distracted driving behavior (e.g. texting, app use) while behind the wheel of a state-owned vehicle.
- d. Expected impact on cost/performance/functionality, etc.
The efficiencies gained in maintenance behavior, vehicle performance, reducing idle time, improving on fuel consumption, route guidance are significant. The ability to score and manage distracted driving behavior and greatly reduce that risk is immeasurable.
- e. Subcontractors/partners involved in delivering service
UScellular partners with READY FLEET to provide this solution. READY FLEET is managed by Ready Wireless and utilizes Modus Telematics as its underlying platform. Custom development and dedicated account support and platform management makes the service a leader in the space.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
READY FLEET addresses all components expected to be included in a Fleet Management platform and more. Location management, maintenance and driver behavior are well represented in a very easy to use and intuitive platform. READY FLEET understands that often the people utilizing the dashboard have many responsibilities outside of vehicle management and safety so creating a solution that's easy to use and able to quickly provide information pertinent to many use-cases was paramount in its design.

Maybe most importantly, the platform has the unique ability to tether an employee's phone to the vehicle via the "cloud" and monitor phone usage behind the wheel. Distracted driving and specifically texting and driving is a serious issue in today's society and knowing how your employees behave behind the wheel is of the utmost importance in risk management. We feel strongly that it is the responsibility of all levels of government to protect the safety of their constituents and having the ability to monitor and manage distracted driving behavior is an elementary step in that direction.

b. Applicability to government needs

See response to "a" above.

c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use. Provide references

There are approximately 250 fleets representing several thousand vehicles and assets currently under management on the READY FLEET platform.

References:

Company	Contact	Title	Phone
Home Town Restyling	Tom Casey	Sales Manager, Partner	(319) 350-9636
Baker Group	Mitchell Wood	Fleet Manager	(515) 314-9478
NIFCO	Cory Richards	Account Manager	(402) 310 5751
AG Electric	Barney Grobstick	President	(563) 590-4056

d. Overall interoperability of turnkey system for government use

READY FLEET operates on an open API platform. Data can either be exported for reporting measures or, with development, the platform can be pointed toward other systems for integration. These efforts would be evaluated under a separate Statement of Work and agreed to mutually before execution.

e. Accessories available for turnkey offering

Outside the normal equipment required to connect the vehicles, there are no other accessories available or required.

As an aside, READY FLEET does not offer or support a camera-based solution for in/out vehicle monitoring. We feel strongly that the data gathered through the platform provides all the actionable data required to manage toward safe driving habits.

READY FLEET does support API integration to a separate ELD provider platform but it's highly unlikely for that to be a requirement for state-owned and mostly locally operated vehicles.

- f. Thoroughness of the vetting process used to select partners
Ready goes through a rigorous process to determine vendor partners. A team of individuals from various departments evaluate each vendor and determine which vendors will be the best fit. This starts with a demo and then based on use cases and scenarios determine if the vendor is able to provide the business requirements needed.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
For new vendor launches and any enhancements the testing process starts with the use cases that were determined and documented for the release. Each use case will be tested several times from multiple users, from various departments, from the beginning of the process to the end of the process within the Quality Assurance environment. Once all parties approve the launch or enhancements with the Quality Assurance environment, the changes will be pushed to the production environment and tested again by multiple users, from various departments, through the entire process for final approval. During both of these phases, any issues would be fixed before approval of that phase and then moving onto the next phase.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package. The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
Client/State will provide an inventory of vehicles and use-cases to determine connectivity and equipment needs. A formal quote specific to those needs will be provided for signature.
- b. Project coordination
READY FLEET will procure equipment if needed and work with onsite fleet management or a 3rd party to coordinate timing and vehicle rotation for installation. Installation of OBD II devices takes mere seconds where 3-wire equipment may take up to 20-30 minutes.
- c. Installation and Testing process
Sample devices will be sent ahead of project implementation for data integrity and trial purposes.
- d. Client Infrastructure and support assessment process
READY FLEET will assign dedicated Account Management personnel to the relationship. Our team will be available to preload vehicle and driver information into the platform, assist with desktop or app support, ensure reporting accuracy and provide ongoing guidance on data trends and actionable items that appear in the platform.

Training sessions will be scheduled for different user levels and ongoing support will be made available.

- e. End user Acceptance process
Our aim is to ensure the end user is gathering the expected data to drive outcomes whether those efforts are maintenance, performance, location or safety driven. Regular interactions (calls, video conferences) will be scheduled to understand and promote acceptance.
- f. Approach to maintenance and support
See response to "d" above.
- g. Initial and Ongoing Training provided
See response to "d" above.
- h. On-going support and enhancement over the life of the agreement
See response to "d" above.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
Embedded in the Fleet Management platform are tools that allow for monitoring of driver behavior, specifically texting and driving. IFTA reporting is a featured component on fuel consumption. Basic dispatch communication is available. And, manufacturer data is also pulled for constant maintenance and recall alerts.

We have found that each of our clients have the ability to identify ways to leverage the data in the solution to better manage not only their vehicle fleet but also their remote working staff as well. Efficiencies are gained in many unique ways and the data is utilized differently depending on the role and end-goals of the user.
- b. Experience and qualifications of partners and subcontractors
READY FLEET has been involved in systems and network integration for over 15 years. Our ability to manage and enable end-to-end solutions is unique in that not only do we have a technical command of the services we put forth, but we support the sales, marketing and ongoing account support effort as well.
- c. Description of Additional Integration and Consulting Services provided
In addition to Fleet Management, READY FLEET hosts a number of risk management and performance-based platforms to help organizations solve complicated problems, simply. Other solutions include but aren't limited to Broadband Failover, Asset Tracking and Management, Contact Tracing and Social Distance Monitoring through LoRa-based technology, Environmental Controls (temp/humidity), Agricultural Solutions and many more.

IoT Management Services Terms and Conditions

Ready Wireless (“READY”) IoT Additional Terms and Conditions are at www.readywireless.com/terms-and-conditions. (“Additional T&Cs”)

In the event of any conflict between the terms of this Agreement, these IoT Management Services T&Cs set forth below, and the Additional T&Cs, the order of priority (high to low) is Agreement, Additional T&Cs and IoT Management Services T&Cs. Without limiting the foregoing, as provided in the Agreement, (i) Your cellular carrier shall bill and collect the Cellular Services Fees from You (“Subscriber” or “Customer”), and (ii) READY will bill and collect the IoT Management Services Fees.

Introduction. READY will use commercially reasonable efforts to provide Customer with “IoT Management Services” requested by You pursuant to the terms of this Agreement, the Additional T&Cs and the IoT Management Services T&Cs

Definitions. “**Device**” means each unique device provisioned and active on the Customer’s cellular network that allows the transfer of data from a motor vehicle and/or asset to READY’s systems, which device may be provided by READY or a third-party or built into the vehicle or attached to the asset. “**IoT Management Services**” include Real Time Location Tracking, Distracted Driving Behavior and Scoring, Customer Alerts and Notifications, Asset Monitoring, and Vehicle Health and Maintenance. The Services are accessed via the Web referred to as the “Fleet or Connect Portal”.

Device Types for IoT Management Services.

- (a) Customer may purchase Devices that are a true plug-and-play device self-installed by the Customer. Fleet Services for such Devices include real-time location tracking, distracted driving behavior and scoring, vehicle health and maintenance, custom alerts and notifications, fleet portals, account management and custom support.
- (b) Customer may purchase Devices that need to be hardwired in the Customer vehicle. Hardware installation is performed by Customer or your cellular carrier’s preferred vendor. IoT Management Services for such hardwired Devices includes all of the plug-and-play Fleet Services listed above, except vehicle health and maintenance services.

Restrictions on Use of IoT Management Services. READY grants Customer the right to access and use the **IoT Management Services** solely for its internal business purposes while this Agreement remains in effect. No license rights are granted (whether by implied license or otherwise) to Customer except as expressly provided in this Agreement and READY reserves all rights not otherwise expressly granted hereunder. Customer shall not, directly or indirectly, (a) copy, license, sell, redistribute, lease or otherwise transfer or assign the **IoT Management Services**; (b) alter or permit a third party to alter any part of the **IoT Management Services**; (c) use or permit the use of the **IoT Management Services** or any Device in the operation of any service bureau or time share services or for any unlawful purpose; (d) disassemble, decompile, reverse engineer or otherwise attempt to derive source code or other trade secrets from the **IoT Management Services** or any Device. Customer may not use the **IoT Management Services** or Device or provide access to the **IoT Management Services** or Device to any person for any purpose prohibited by law. Customer shall ensure all third parties to which it provides access to the **IoT Management Services** or any Device adhere to the terms of this Agreement. Customer agrees to notify READY immediately in writing in the event any unauthorized access, disclosure, distribution, possession, alteration, transfer, reproduction or use of the IoT Management Services is found.

Data. In the course of providing the **IoT Management Services**, READY may receive or collect data relating to the Customer vehicles and/or assets in which a Device is installed or data related to the owners, operators and occupants of such vehicles and/or assets, including GPS information, vehicle speed, acceleration, hours of operation of the vehicle, vehicle identification number (VIN), vehicle diagnostics information, materials being transported by the vehicle, and information related to employees, contractors and suppliers of Customer (e.g., names and identification numbers of employees and operators of vehicles of Customer) (collectively, “Collected Data”), temperature, performance, capacity, fill rate, volume, and vibration. Customer agrees that while IoT Management Services are provided, and following the termination or expiration of this Agreement, READY will have the right to: (i) use Collected Data in order to provide **IoT Management Services** pursuant to this Agreement, including responding to comments and questions from Customer and implementing the **IoT Management Services**; (ii) use Collected Data to conduct research and development activities, including further developing READY’s services and products; (iii) disclose Collected Data to third parties providing services to READY and permit such third parties to use the

Collected Data in connection with such IoT Management Services;

(iv) disclose Collected Data if required under applicable law, regulation or court order; (v) use and disclose the Collected Data to protect, investigate and deter against fraudulent, unauthorized, or illegal activity; and (vi) use and disclose Collected Data for other purposes so long as the Collected Data is used in an aggregated fashion such that the source of the Collected Data cannot reasonably be identified.

Vehicle-and/or Asset Related Consent. When a Device is installed in a vehicle and/or Asset pursuant to this Agreement, Customer is solely liable to ensure the vehicle is under its authority to receive such Fleet Services.

Security Measures. READY will use commercially acceptable practices to implement technical, administrative, and physical security measures that are designed to protect the **IoT Management** Services from unauthorized access, use or modification. From time to time, READY reviews its security procedures to consider appropriate new technology and methods. However, despite READY's commercially reasonable efforts, no security measures are perfect or impenetrable.

IoT Management Services Area. Customer acknowledges that the **IoT Management** Services are intended and made for exclusive use only within the continental United States. READY makes no representation that the **IoT Management** Services are appropriate or available for use in other locations outside the continental United States. As READY bundles the wireless service within the **IoT Management** Services, Customer may use the wireless service solely in connection with the **IoT Management** Services within such service area of such wireless carrier and will not otherwise misuse the wireless service (e.g., take the vehicle and/or asset outside the carrier service area or insert a SIM card, if applicable, into another device).

Customer Acknowledgements. Customer acknowledges that READY may not be able to provide the **IoT Management** Services at all times due to reasons outside of READY's control, including if: i. the Device and/or Asset is not (A) connected to an appropriate power source or cellular network, (B) transmitting or receiving data or where data functionality is otherwise impaired, or (C) incorrectly installed in the vehicle or is not properly functioning; ii. the Device and/or asset is not active on your cellular carrier's network or there is a failure of cellular networks or any hardware outside the reasonable control of READY; iii. the vehicle operator has manually overridden the functioning of the Device; or iv. the vehicle driver identification function has not yet been completed. Customer may only use a Device with a compatible vehicle and/or asset.

Customer acknowledges that the Device uses a certain amount of current from the battery even when the vehicle is not turned on. Care should be taken in using the Device in vehicles that have old or weak batteries, or that may go extended periods without being started. Customer shall not use the Device or Fleet Services in or with motor vehicles with a modified engine, modified electronic control systems, or cars of any make, model or year that are not supported.

Such use shall be deemed nonconforming and inappropriate use of the **IoT Management** Services and in violation of this Agreement. READY will not be liable for nonconforming and inappropriate use of any Device or **IoT Management** Service. READY, in its sole discretion or at the instruction of the applicable wireless provider, may from time to time make additions to, deletions from or modifications to the **IoT Management** Services and the equipment, software or communications facilities used to provide and receive the **IoT Management** Services. READY shall make commercially reasonable efforts to notify Customer upon adoption of such modifications, except that changes not materially affecting Customer's use of the **IoT Management** Services and minor changes may be adopted without providing Customer with notice to that effect. Continued receipt or use by Customer of the **IoT Management** Services after any modification shall constitute Customer's acceptance of such modification.

READY Portal and License to Use. READY shall make a web portal and related documentation available to Customer for use in connection with the **IoT Management** Services (the "Portal"). READY grants to Customer a non-exclusive, revocable, non-transferable and non-sublicensable right to use the Portal solely for use in connection with the **IoT Management** Services while this Agreement remains in effect solely for Customer's own internal business purposes and subject to Customer's payment of all fees due and payable under the Agreement. The READY Portal and related documentation are Confidential Information of READY (excluding, for clarity, any data or content provided by Customer for use on the READY Portal). Customer shall only permit its authorized employees and agents who have agreed in writing to comply with the terms of this Agreement, to access and use the READY Portal (each an "Authorized User"). Customer shall be responsible for all acts and omissions of any individual who accesses a READY Portal on behalf of Customer or utilizes Customer equipment or who use log-in information provided or made available to Customer by READY. Customer shall promptly (but in any event within twenty-four hours) notify READY of any unauthorized use of a READY Portal or any other known or suspected breach of security related to the READY Portal. All rights of READY and its licensors in intellectual property not expressly granted to Customer are reserved by READY and its licensors. Customer shall cease all use of a READY Portal upon the expiration or termination of this Exhibit or, if applicable, the Phase Out Period. READY will create accounts for a reasonable number of Authorized

Users with a unique user name and password. Customer shall cause Authorized Users to only use these credentials to log in and access the READY Portal in accordance with the requirements of this Agreement. Customer shall be responsible for identifying all of its Authorized Users, for approving access by its Authorized Users to the READY Portal, for controlling against unauthorized access by such Authorized Users, and for maintaining the confidentiality of the user names, passwords and account information for all Authorized Users accounts. Customer shall be responsible and liable for (and READY shall not be responsible or liable for) any activities that occur under Customer's or its Authorized Users' accounts or passwords or as a result of Customer's or Authorized Users' access to the READY Portal, including any actions or omissions by individuals accessing a Customer or Authorized User account without authorization. Furthermore, Customer agrees not to transmit or store infringing, obscene, threatening, libelous, or otherwise unlawful or offensive content or other materials or information that violates the privacy rights of any person or to transmit or store material containing software virus, worms, trojan horses or other harmful computer code or malware when using the READY

Portal. Customer shall abide by all applicable local, state, national and international laws and regulations in connection with Customer's use of the READY Portal, including those related to taxes, data privacy and the transmission of technical or personal data. READY shall not be liable or responsible for the deletion, correction, destruction, damage, loss or failure to store any data or content of Customer located on the Portal. Customer shall be fully responsible for all internet access and connectivity requirements to (and resolving any issues that arise in connection with) access the READY Portal.

Customer acknowledges and agrees that READY owns all right title and interest in and to the READY Portal (excluding, for clarity, any data or content provided by Customer for use on the READY Portal) and any derivative works thereof, and no license to the READY Portal is granted to Customer by implication, estoppel or other than as expressly set forth in this Exhibit. Customer agrees not to: (i) remove or modify any trademark, service mark, copyright or other notice of READY's or its licensors' proprietary rights; (ii) modify, make derivative works of, disassemble, reverse compile, reverse engineer, reproduce, or download any part of the READY Portal, including any software of documentation to which Customer is provided access in connection with the READY Portal; (iii) conduct any benchmark tests or performance tests of the READY Portal without READY's prior written consent and participation; or (iv) sublicense, sell, rent, lease, transfer, assign, distribute, display, disclose, republish, make or permit timesharing or service bureau use or use for any unlawful purpose, or otherwise commercially exploit or make the READY Portal, including any software of documentation to which Customer is provided access in connection with the READY Portal, available to any third party.

Indemnification. In addition to the indemnification set forth in the Additional T&Cs, Customer will defend, indemnify, and hold READY and its affiliates and their respective officers, directors and employees harmless from and against all claims, complaints, losses, costs, and expenses (including reasonable attorneys' fees) (collectively "Claims") asserted by third parties that are not affiliates of READY to the extent arising out of or in connection with (a) the IoT Management Services or any Device (and, for clarity, regardless of whether the IoT Management Services or READY's breach of the Agreement or negligence contributed to such Claims), (b) any libel, slander, or infringement of copyright arising from the material transmitted using the IoT Management Services or any Device; or (c) the combination, integration, or incorporation of the IoT Management Services with a device, product or service not provided by READY. The indemnification procedures set forth in the Additional Terms shall apply with respect to any claim for indemnification under this section.

Notices. All notices and other communications required or permitted hereunder shall be in writing and shall be mailed by certified or registered mail (return receipt requested), or overnight express air courier, charges prepaid, addressed as follows to READY and to the address provided by Customer, and such notices will be deemed to be made when actually received:

READY WIRELESS, LLC
955 Kacena Road, Suite A
Hiawatha, IA 52233
Attention: Legal Department

If to Customer:

COMPANY NAME	
ATTENTION	
ADDRESS	
CITY, STATE	
ZIP	

.

Device Warranty and Refund Policy

READY offers a limited warranty on devices and modules (collectively, the “Device”). If you believe the Device you received is defective, please notify READY as soon as possible and provide sufficient detail to justify your claim. If a Device is determined to be defective in the reasonable discretion of READY, a refund or a replacement (providing stock of the exact make/model/color/condition is available) will be offered if READY is contacted within the specified warranty period noted below.

Please contact your cellular carrier Representative and READY for a RMA # (Return Merchandise Authorization) prior to returning or exchanging any item. Obtaining a RMA# is the only way to ensure a refund or exchange will be processed. You must ship your item within 30 days of receiving your RMA# in order to receive a refund or replacement. Please do not send your purchase back to the manufacturer.

Refunds (if applicable)
Once your return is received and inspected, if approved, your refund will be processed. READY does not offer a refund for the shipping costs incurred upon purchase of the Device. The Device being returned must be received in the same condition as when it left the READY facility. If the returned item is missing any internal stickers or serial number information, a refund will not be issued. Refunds are issued to the same account that the purchase was made from

Exchanges (if applicable)
READY will only replace a Device that is defective, as reasonably determined by READY in its sole discretion. This policy does not apply to breakage caused by Customer negligence or water damage. Once your return is received and inspected, your request will be promptly processed. If there is a problem with your order, please contact READY at 1-800-570-3869 during the below hours of operation:

Monday – Friday 7:30 am to 5:00 PM (CST)

If there seems to be a mechanical, electrical, or programming problem with your Device, DO NOT attempt to repair or try to unlock it yourself or take it to a third party for repair without first contacting READY. Doing so will automatically void any applicable warranty. READY does not reimburse you for third party repairs or purchases. READY shall make all commercially reasonable efforts to ensure that the Device received is as described.

Warranty Term	
Device	Warranty Term
Device (new)	12 Months from ship date to Customer

IOT MANAGEMENT SERVICES AGREEMENT, IoT MANAGEMENT SERVICES TERMS & CONDITIONS, READY’S ADDITIONAL T&CS, AND WARRANTY POLICY ARE ACCEPTED BY CUSTOMER. :

NAME:

TITLE:

SIGNATURE:

DATE:

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh
Subcategory A: Fleet Management

Client Company name:	Gold Eagle Cooperative
Client name of contact:	Tully Waddingham
Client contact title:	Director of Technology
Client is a daily user, occasional user, etc.:	Daily User

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to James Rose no later than Friday, November 6th.

Thank you for your assistance in this process.

- 1. For what services do you use USCC's product, and how long have you been USCC's customer?**
Cellphones, tablets, GPS Trackit
- 2. Would you recommend USCC to other customers? Why?**
Yes, great network, customer service, and response time.
- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

Brought out a team, was well coordinated, and implementation went seamless. Out of everything US Cellular has to offer we are most pleased with response time. They have never missed a deadline.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

Yes, customer service is spot on. They haven't disappointed us to date.

- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

Most drivers absolutely love it, but we are having users push back as well that aren't technology savvy.

- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

Overall, we have no complaints.

- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

Great company and thoroughly impressed if any issues arise.

- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

Cellphones and tablets and cell boosters within buildings.

Attachment D:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh
Subcategory A: Fleet Management

Client Company name:

Sho-Me Power Electric Cooperative

Client name of contact:

Micah Johnson mjohnson@shomepower.com

Client contact title:

Manager, IT Infrastructure

Client is a daily user, occasional user, etc.:

Daily

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to James Rose no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

MiFleet AVL - little over 2 years.

2. Would you recommend USCC to other customers? Why?

Yes, our experience has been that they met our need at a price point that is lower than their competitors.

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

Everything went as expected.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

No disappointments, met expectations.
- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

Works exactly as expected. Exceeded in that we can use it in ways that we could not with prior product.
- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

N/A no changes at all.
- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

N/A
- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

One smart phone

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory A: Fleet Management

Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)

Client Company name:

Knoxville-Knox County Head Start

Client name of contact:

Lisa Silverman & Jodie Fain

Client contact title:

Data Integration Manager & Program Manager

Client is a daily user, occasional user, etc.:

Administrators Daily User

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Jim Cosmos no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

- Customer with USC for 15 or more years
- Cellular phones (iPhones), tablets with data (LG G5 & Samsung Galaxy Tab A), Ready Fleet Vehicle Monitoring & IBM Maas 360

2. Would you recommend USCC to other customers? Why? YES

- Always responsive to our needs
- Have a yearly meeting to discuss our current service and rates
- USCC has made recommendations about things we need to do to lower our bill
- USCC monitors the data usage and will make suggestions regarding plans
- USCC has helped KKCHS to meet several needs of the program
- KKCHS wanted smart phones for all classrooms however, we could not afford the monthly data plans. USCC created a plan where all classrooms could have a smart phone without data. The phone is able to connect to Wi-Fi at each location and the smart phone can be used. This is at a much lower cost than a data plan for each smart phone.
- USCC was able to work out the purchasing of tablet cases for each of the tablets.

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

- In the beginning of the IBM Maas 360, USCC had at least 3 meetings with KKCHS, USCC and IBM on the installation of the program.
- With the purchase of an initial 400 tablets, USCC enrolled all tablets in the program.
- The additional delivery of our purchase of 200 tablets was timely and USCC assisted with the installation of the IBM Maas360, as well as providing written instructions to install, update and reset IBM Maas360 on the tablets.
- USCC delivered all tablets in the time frame that was initially presented.

4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?

- USCC has always been extremely customer service oriented.
- USCC responds very quickly to emails, texts, and calls.
- USCC will come on site and work to help implement new devices and software.

5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?

- Yes, the IBM Maas360 worked the way USCC initially presented it to KKCHS.
- It has met the expectations of KKCHS.

6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?

- The relationship with USCC has been superb as it has been in the past.

- One thing that we wish we had was a clearer understanding of how the IBM Maas360 was going to work for our KKCHS end user (Head Start / Early Head Start Parents).

7. Is there anything else you think we should know about working with USCC or using USCC's products and services?

- USCC has been extremely responsive and supportive to the inquiries and needs of KKCHS.

8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?

- iPhones (in excess of 100)
- Tablets (LG G 5 – 670)
- Tablets (Samsung Galaxy Tab A --- 65)
- Ready Fleet Monitoring Units (44)
- IBM Maas360 (600)
- KKCHS does not have any other relationships with USCC other than what is listed above.

Appendix E

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

**Subcategory B: Mobile Device Management /Enterprise
Mobility Management (MDM/EMM)**

MaaS360 by IBM



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
MaaS360 by IBM
- b. General Application Area
Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)
- c. General capabilities provided
MaaS360 by IBM is a secure & comprehensive mobile device management (MDM) or enterprise mobility management (EMM) platform that is easy to deploy and scale for medium and enterprise business and government customers across any and all industries. Using MaaS360, organizations can manage and safeguard their mobile devices, apps and content with flexible solutions to help meet their specific needs. In an era of growing Bring-Your-Own-Device (BYOD) use policies, MaaS360 helps businesses and government entities ensure their employees have the apps and content that they need to be productive, while maintaining data security and personal privacy.

Key Capabilities:

- Manage Entire Mobile Device Fleet
 - iOS, Android, Windows Phone, BlackBerry, Windows & OS X
 - Over-the-air (OTA) configuration, security policy enforcement, locate & selective wipe, jailbreak & root detection, geofencing, automated compliance engine
 - Integrate with Exchange, Lotus Notes, Office 365, AD/LDAP, BES & certificate authorities
- Increase Productivity with Secured Emails, Apps & Docs
 - Complete set of office productivity tools for secure viewing, editing & sharing from content repositories like SharePoint
 - Enterprise app catalog for 3rd party & in-house apps
 - App security and compliance policies, including blacklisting, whitelisting & authentication
- Reduce Security & Compliance Risks
 - Trusted WorkPlace container with a dual persona approach to separate work from personal mobile data
 - Data leak prevention controls to restrict sharing, copy, paste, screen capture & more
 - Mobile malware detection, analysis & remediation
- Control Entire Mobile IT Environment
 - Complete, real-time visibility with MaaS360 dashboard
 - Automated compliance & rules enforcement engine
 - Mobility Intelligence analytics, reporting & action engine
- d. Expected impact on cost/performance/functionality, etc.
The 5 key benefits of using MaaS360 to deliver value to the organizations by managing and securing mobile environment include:
 - 1. Easily manage devices
 - See all devices in one place and remotely manage right over-the-air (OTA)
 - 2. Quickly deploy private and public apps
 - Promote, distribute and update approved apps using an interactive catalog
 - 3. Collaborate with content on-the-go

- Mobilize content and files to stay productive anytime, anywhere
- 4. Keep apps and data secure
 - Help users get the information they need without risk of data leakage
- 5. Simply connect to business systems
 - Integrate with enterprise systems to use existing infrastructure and data repositories

MaaS360's most important cost benefit is its positive impact on ROI (return on investment). Some examples on various industries are below:

- A healthcare organization using MaaS360 reduces mobile health desk tickets on average of 1/8
 - A leading gaming and entertainment company reduces customer wait time by 80% with tablets using a single managed app to speed the time to deliver food and drinks to customers
 - A large U.S. children's hospital protects 3,000+ mobile devices ensuring HIPAA compliance; installed and integrated with existing servers in just 90 minutes
- e. Subcontractors/partners involved in delivering service
IBM – US Cellular distributes the MaaS360 service via a “bill on behalf” model.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
N/A

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
MaaS360 delivers secure enterprise productivity across three areas, each component of which working harmoniously with one another:
- 1) Secure access:
 - Data containerization via secure productivity apps
 - Contextual access & single sign-on (SSO) to cloud apps
 - Multi-factor authentication
 - 2) Data protection:
 - Configuration-based malware detection
 - Secure browsing with global threat intelligence
 - Device-agnostic, network-based protection
 - 3) Enterprise visibility:
 - Visibility into any endpoint located anywhere
 - Intelligent policy & compliance rule creation
 - Advanced threat detection and remediation

- b. Applicability to government needs
MaaS360 supports 50,000+ customers globally with environments ranging from 5-500,000 devices including government and state entities. Regardless of industry and vertical, MaaS360's capabilities are applicable to wide range of organization needs including government.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use. Provide references
MaaS360 supports 50,000+ customers globally with environments ranging from 5-500,000 devices including government and state entities. US Cellular on its own provides the proposed service to more than 170 customers with approximately 11,500 licenses. School District of Janesville, WI is a reference customer – see testimonial.
- d. Overall interoperability of turnkey system for government use
Our mobile device management solution MaaS360 from IBM is well-suited for government use – see testimonial from School District of Janesville, WI.
- e. Accessories available for turnkey offering
MaaS360 comes as Software as a Service (SaaS) and works on mobile devices such as smartphones and tablets, laptops and expanding into wearable technologies and IoT (internet of things) components.
- f. Thoroughness of the vetting process used to select partners
A thorough industry analysis and full RFP process were used to select IBM as UScellular's solution provider. IBM has been recognized as a leader in Enterprise Mobility Management (EMM) by respected industry analysts, including Gartner and Forrester. IBM is a "Leader" in the Magic Quadrant for EMM for 4 years in a row and earned the title "best-in-class cloud among ranked EMM vendors.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
The MaaS360 solution from IBM has been tested in both UScellular and IBM labs for integration with related US Cellular solutions, such as UScellular provided mobile devices (Android and IOS smartphones, tablets etc.). The solution is in use both internally and deployed with many US Cellular customers.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package. The description included in the proposal will be scored based on the suitability of the plan to government needs.

IBM will manage the customer experience from end to end. This includes, but is not limited to: presenting the offer, completing the sale, setting up the account, installing the software, billing, and supporting all account activities. The professional implementation team uses a consultative design approach and collaborative process, with one specialist assigned to the customer, from launch to completion.

- a. Pre-installation coordination
Response above.
- b. Project coordination
Response above.

- c. Installation and Testing process
[Response above.](#)
- d. Client Infrastructure and support assessment process
[Response above.](#)
- e. End user Acceptance process
[Response above.](#)
- f. Approach to maintenance and support
[Response above.](#)
- g. Initial and Ongoing Training provided
[Response above.](#)
- h. On-going support and enhancement over the life of the agreement
[Response above.](#)

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
[MaaS360 customers can reach out to their MaaS360 account executive to begin the technical support process. They can also contact the technical support team directly via the live chat option on their MaaS360 app, or email and phone.](#)
- b. Experience and qualifications of partners and subcontractors
[See response to "a" above.](#)
- c. Description of Additional Integration and Consulting Services provided
[See response to "a" above.](#)

Appendix I

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

**Subcategory B: Mobile Device Management /Enterprise
Mobility Management (MDM/EMM)**

Scalefusion



1 - General information:

Please provide a general description of the solution you are offering including:

a. Product Name

Scalefusion

b. General Application Area

Subcategory B: Mobile Device Management and Enterprise Mobility Management

c. General capabilities provided

A cloud-based Device Management solution that does much more than just managing and securing Employee-Owned (BYOD) and/or Company-Owned Devices, unlocking the true enterprise mobility potential with finesse.

The solution can be used in any domain that involves the usage of mobile devices, tablets and/or laptops (Mac, Windows).

- Multiplatform device management
- Various types of policies – Company Owned Device (Single Purpose and Personally enabled), Bring Your Own Device, Agent mode, Kiosk Mode
- Apps & Content Management
- Secure Browsing
- Communication tools to stay connected – One Team (sold separately)
- Android Zero-Touch and Apple DEP for Out-of-the-box experience, along with deployment on a large scale without having to configure every single device
- Exchange, GSuite and Office 365 login capabilities (SSO)
- Cloud storage for secure and easy access of files of every type
- Workflow automation to ensure compliance and security
- Single Pane of Window (Dashboard) for comprehensive view of devices and policies
- Multiple admins with definition for roles & privileges
- Geo-fencing capabilities
- Remote Cast and Control (for specific devices) to assist remotely
- Custom APIs available for integration
- ITSM tool integration for ticket management
- FREE 24 x7 support
- License reusability when device is lost, or employee leaves the organization

d. Expected impact on cost/performance/functionality, etc.

Security/Data breach can cost companies millions of dollars and solutions like MDM/EMM ensure that the corporate devices are secure, compliant and remotely manageable when compromised. With the increase of remote working and remote workforce, the challenges to make sure necessary apps are distributed across various platforms and devices is unsurmountable. Scalefusion ensures easy and quick ways to distribute apps and content while ensuring device security whether employee or company owned.

- e. Subcontractors/partners involved in delivering service

We are regional partners with Scalefusion which has office presence in India, Canada, Mexico. We have rolled out the MDM/EMM solution to clients who have seen the benefits and are sleeping peacefully as security is ensured.

- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.

Yes. Please see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described

The product is a self-service easily scalable and economical cloud-based service. As a multi-platform solution, the product caters to various devices and device policies or a mix of them as required by businesses.

- Remote Cast & Control (RCC) – Ability to resolve device and/or app issues for a perimeter-less office is very difficult. RCC lets your system administrator remotely connect with a device troubleshoot and/or reset policies in the quickest possible way; reducing both time and cost of shipping as well as providing a replacement device.
- EVA Communication suite – Ability to communicate with the office, managers and colleagues is an inherent need even when the devices are governed by policies. Public tools and messengers may allow organizational data to be compromised. A secure text messaging tool along with VOIP calling abilities makes it easier for employees and the office to stay in touch all the time!
- License reusability – Many solutions that are in the market do not allow for reusability of licenses when a device is lost, or an employee leaves the organization. Our solution allows for reuse of licenses in both the scenarios increasing the value for the investment made with the MDM/EMM
- Self Service platform – Easy to use dashboards and intuitive guides allow system administrators to use the platform without any external consultant need. Additional costs on consultants and/or admins is not required to administer the solution to employees on both small and large scales
- ITSM Integration – Device and defect details are available on the MDM/EMM platform. Integrating a ticket/service management tool allows to effectively track and resolve issues and caters to build a knowledge repository. Our solution can integrate any token based authenticated ITSM tool like ServiceNow or FreshService to raise and manage tickets from within our dashboard!
- Support – This is one of the most defining moments of truth for any software or solution. We are rated highest in G2Crowd and Gartner for customer support and service. We have received several awards for customer service and support over the last few years.

- b. Applicability to government needs

The solution is domain agnostic and is ISO 270001 compliant and should cater to all the needs of government from both functional and security perspective.

- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
The solution has about 4500+ global customers including half a million devices from various platforms and devices. With a 5 Star rating on G2Crowd and Capterra with consistent leadership position in the customer service and support space, our MDM/EMM solution is definitely the best ROI you will ever receive.
- d. Overall interoperability of turnkey system for government use
The solution is domain agnostic and integrable with various application areas including government.
- e. Accessories available for turnkey offering
With EVA communication suite and One Team organizations can handle device deployments for field activities at scale without having to worry about bloating costs or infrastructure needs.
- f. Thoroughness of the vetting process used to select partners
A globally renowned solution with sizeable footprint across the world ensures the solution is robust and the best investment for any organization.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
Client partners ensure they carry out their rigorous testing suites to ensure functionality, scalability and security of our MDM/EMM solution.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
 - Device types and configurations are to be shared in a predefined excel format
 - System admin handholding and training will be done for first 100 devices from where the organizations can switch to autonomous mode
 - Device policies for various organization groups have to be defined along with the type of device policies (COPE, BYOD, Agent, Kiosk, etc.)
- b. Project coordination
Goldie Group will facilitate all liaison for the deployment of the solution successfully and will ensure all the devices are deployed and running in the first iteration/phase of the operations. Goldie and Scalefusion Support teams will be available to answer and/or troubleshoot queries at any point in time.
- c. Installation and Testing process
 - Device policies along with app and content will be deployed to the enrolled devices
 - Sanity tests will be conducted to ensure policies are deployed appropriately
 - Integration if applicable will be worked appropriately with the client partner to ensure smoother operations.

- d. Client Infrastructure and support assessment process
 - Intercom integration on the dashboard is available for ready and quick answers for common problems
 - Support personnel answer questions ensuring reliable resolutions
 - 24 x 7 support is available during workdays and holidays/weekends are supported on a need/criticality basis
- e. End user Acceptance process
 - Goldie and Scalefusion work with client to ensure device policies are deployed along with application download
 - Sanity checks of a few devices are conducted to ensure smooth operations
- f. Approach to maintenance and support
 - Support and maintenance with zero effect on end users is ensured.
 - Zero down time for end-users with minimal downtime for system admins (in accessing dashboard) during patch, security and feature updates.
- g. Initial and Ongoing Training provided
 - Initial hand holding, and device deployments will be assisted
 - Ongoing training for new features is conducted on a regular basis
 - Ongoing support can be purchased, and our Business Analysts work remotely or on-premises to hand hold the teams.
- h. On-going support and enhancement over the life of the agreement
 - Free updates and feature inclusions are covered as part of the license agreement
 - Support is included in the licensing cost. On-premises support is chargeable.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
 - Separate document on SLAs will be shared on a need basis once we are onboard with client partners. This shall detail availability, uptime, and other insurance measures to ensure smooth business operations
- b. Experience and qualifications of partners and subcontractors
 - Goldie Group celebrates a 30+ year experience and knowhow in operations, warehousing, distribution and servicing technology needs for clients. Scalefusion is a young and dynamic solution company with more than 6 years of experience and several years of technical know-how.
- c. Description of Additional Integration and Consulting Services provided
 - On a need basis Goldie Group shall develop custom software and solutions that are required to augment the current business operations of the client.
 - Our current supply chain platforms and back end integrations will also come in use for the large-scale deployment in disparate geographies.

Scalefusion MDM: Unified Device & Endpoint Management Solution

Terms of Service

Version: 4.0

Effective Date: 1 February, 2020

This “**Scalefusion (formerly MobiLock Pro)**” Terms of Service Agreement (the “Agreement”) is between you and ProMobi Technologies Pvt Ltd (India - U74900PN2014PTC150210) (“ProMobi”). If you are agreeing to this Agreement not as an individual but on behalf of your company, then “Customer” or “you” means your company, and you are binding your company to this Agreement. ProMobi may modify this Agreement from time to time, subject to the terms in Section 16.7 (Changes to this Agreement) below.

By clicking on the “I agree” (or similar button/link/checkbox) that is presented to you at the time of your Order, or by using or accessing ProMobi products, you indicate your assent to be bound by this Agreement.

Scope of the Agreement: This Agreement governs your initial purchase as well as any future purchases made by you that reference this Agreement. This Agreement includes our [Privacy Policy](#), our [Acceptable Use Policy](#), any Orders, and any other referenced policies and attachments. This Agreement applies to Scalefusion add-ons or plugins that you purchase from the Scalefusion website or from authorised resellers and distributors. However, it does not apply to apps, add-ons or plugins from other vendors that you install on your managed devices.

The “**Effective Date**” of this Agreement is the date which is the earlier of (a) Customer’s initial access to any Service (as defined below) through any online provisioning, registration or order process or (b) the effective date of the first Order Form referencing this Agreement.

As used in this Agreement, “ProMobi” means (a) ProMobi Technologies Pvt. Ltd., an Indian corporation with registered office at 303, Welworth Classic PLNo:2+3, SNo: 22/2, Wadgaonsheri, Pune, MH 411014, India.

ProMobi Products: This agreement governs (A) ProMobi’s software subscriptions to online software-as-a-service products

Account Registration

Revisions to this agreement: From time to time, ProMobi may modify this Agreement. Unless otherwise specified by ProMobi, changes to this term will be effective upon renewal of Customer’s current Subscription Term (as defined below) or entry into a new purchase order form. ProMobi will use reasonable effort to inform Customer of the changes through communications via Customer’s account, email or other means. In some cases Customer may be required to click to accept the new

terms or otherwise agree to the modified agreement before renewing the Subscription Term or entering into a new purchase order form, and in any event continued use of the ProMobi's products or services after the updated terms of this Agreement goes into effect will constitute Customer's acceptance of such updated terms. If ProMobi specifies that changes to the new terms will take effect prior to Customer's next renewal or purchase order (due to legal compliance or product change reasons) and Customer objects to such changes, Customer may terminate the applicable Subscription Term and receive as its sole remedy a refund of any fees Customer has pre-paid for use of the applicable Services for the terminated portion of the Subscription Term.

BY INDICATING YOUR ACCEPTANCE OF THIS AGREEMENT OR ACCESSING OR USING ANY SERVICES, YOU ARE AGREEING TO BE BOUND BY ALL TERMS, CONDITIONS, AND NOTICES CONTAINED OR REFERENCED IN THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, PLEASE DO NOT USE ANY SERVICES. FOR CLARITY, EACH PARTY EXPRESSLY AGREES THAT THIS AGREEMENT IS LEGALLY BINDING UPON IT. THIS AGREEMENT CONTAINS MANDATORY ARBITRATION PROVISIONS THAT REQUIRE THE USE OF ARBITRATION TO RESOLVE DISPUTES, RATHER THAN JURY TRIALS. PLEASE READ IT CAREFULLY.

1. Definitions

“Scalefusion (formerly MobiLock)” or “Scalefusion (formerly MobiLock Pro)” means a proprietary Enterprise Mobility Management solution developed, owned and marketed by ProMobi as software-as-a-service solution. In this agreement it will further be referred as **“Scalefusion”** only.

“Affiliate” means any entity under the control of Customer where “control” means ownership of or the right to control greater than 50% of the voting securities of such entity.

“AUP” means ProMobi's [Acceptable Use Policy](#).

“Contractor” means an independent contractor or consultant who is not a competitor of ProMobi.

“Customer Data” means any data of any type that is submitted to the Services by or on behalf of Customer, including without limitation: (a) data submitted, uploaded or imported to the Services by Customer (including from Third Party Platforms) and (b) data provided by or about People (including chat and message logs) that are collected from the Customer use of the Services.

“Customer Properties” means Customer's devices, apps, files owned and operated by (or for the benefit of) Customer through which Customer uses the Services to manage their account and devices.

“Dashboard” means Scalefusion's user interface for accessing and administering the Services that Customer may access via the web or the Scalefusion Apps.

“Documentation” means the technical user documentation provided with the Services.

“Feedback” means comments, questions, suggestions or other feedback relating to

any ProMobi product or service.

“ProMobi App” means any mobile application or desktop client software included in the applicable Service that is made available by ProMobi.

“Laws” means all applicable local, state, federal and international laws, regulations and conventions, including, without limitation, those related to data privacy and data transfer, international communications, and the exportation of technical or personal data.

“People” (in the singular, “Person”) means Customer’s end user customers, potential customers, and other users of and visitors to the Customer Properties.

“Permitted User” means an employee or Contractor of Customer or its Affiliate who is authorized to access the Service.

“Sensitive Personal Information” means any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards (“PCI DSS”); (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (“HIPAA”); or (iii) any other personal data of an EU citizen deemed to be in a “special category” (as identified in EU Data Protection Directive 95/46/EC or any successor directive or regulation).

“Services” means ProMobi’s proprietary software-as-a-service solution(s), including the Dashboard, Scalefusion application programming interfaces (APIs), Scalefusion Code and Scalefusion Add-on Apps, Scalefusion JavaScript APIs, Scalefusion Developer APIs as described in the applicable purchase order form.

“Taxes” means any sales, use, GST, value-added, withholding, or similar taxes or levies, whether domestic or foreign, other than taxes based on the income of ProMobi.

“Third-Party Platform” means any software, software-as-a-service, data sources or other products or services not provided by ProMobi that are integrated with Services as described in the Documentation.

2. ProMobi Services

2.1. Services Overview: ProMobi’s Services are a suite of mobility software-as-a-service solutions offered through a single platform. The Services are designed to enable Customer to manage their corporate owned devices and to provide a Dashboard for accessing and managing Customer Data regarding those devices. Customer may import and export Customer Data between the Services and certain Third-Party Platforms through supported integrations. The Services also include ProMobi Apps or Code deployed on Customer Properties (i.e devices) to enable management functionality.

2.2. Provision of Services: Each Service is provided on a subscription basis for a set term designated on the purchase order form (each, a “Subscription Plan”). ProMobi may also offer Professional Services (as defined in Section 11) related to certain Services. Customer will purchase and ProMobi will provide the specific Services and related Professional Services (if any) as specified in the applicable purchase order form.

2.3. Access to Services: Customer may access and use the Services solely for its own benefit and in accordance with the terms and conditions of this Agreement, the Documentation and any scope of use restrictions designated in the applicable purchase order form (including without limitation the number of devices managed). Use of and access to the Services is permitted only by Permitted Users. If Customer is given API keys or passwords to access the Services on ProMobi's systems, Customer will require that all Permitted Users keep API keys, user ID and password information strictly confidential and not share such information with any unauthorized person. User IDs are granted to individual, named persons and may not be shared. If Customer is accessing the Services using credentials provided by a third party (e.g., Google), then Customer will comply with all applicable terms and conditions of such third party regarding provisioning and use of such credentials. Customer will be responsible for any and all actions taken using Customer's accounts and passwords. If any Permitted User who has access to a user ID is no longer an employee (or Contractor, as set forth below) of Customer, then Customer will immediately delete such user ID and otherwise terminate such Permitted User's access to the Service. The right to use the Services includes the right to deploy ProMobi Apps and Code on Customer Properties in order to enable device management, monitoring and similar functionality and to collect Customer Data for use with the Services as further described below.

2.4. ProMobi Apps: To the extent ProMobi provides ProMobi Apps for use with the Services, subject to all of the terms and conditions of this Agreement, ProMobi grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to use the object code form of the ProMobi Apps internally, but only in connection with Customer's use of the Service and otherwise in accordance with the Documentation and this Agreement.

2.5. Deployment of ProMobi Apps: Subject to all of the terms and conditions of this Agreement, ProMobi grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to deploy the ProMobi Apps in the form provided by ProMobi on Customer Properties solely to support Customer's use of the Service and otherwise in accordance with the Documentation and this Agreement. Customer must install ProMobi Apps on the Customer Properties in order to enable features of the Services. Customer will deploy all ProMobi Apps in strict accordance with the Documentation and other instructions provided by ProMobi. Customer acknowledges that any changes made to the Customer Properties after initial deployment of ProMobi Code may cause the Services to cease working or function improperly and that ProMobi will have no responsibility for the impact of any such Customer changes.

2.6. Contractors and Affiliates: Customer may permit its Contractors and its Affiliates' employees and Contractors to serve as Permitted Users, provided Customer remains responsible for compliance by such individuals with all of the terms and conditions of this Agreement, and any use of the Services by such individuals is for the sole benefit of Customer.

2.7. General Restrictions: Customer will not (and will not permit any third party to): (a) rent, lease, provide access to or sublicense the Services to a third party; (b) use the Services to provide, or incorporate the Services into, any product or service provided to a third party; © reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to the Services, except to the extent expressly permitted by applicable law (and then only upon advance notice to ProMobi); (d) copy or modify the Services or any Documentation, or create any

derivative work from any of the foregoing; (e) remove or obscure any proprietary or other notices contained in the Services (including without limitation (i) the “Powered by Scalefusion” designation that may appear as part of the deployment of the Services on Customer Properties and (ii) notices on any reports or data printed from the Services); or (f) publicly disseminate information regarding the performance of the Services.

2.8. Scalefusion APIs: If ProMobi makes access to any APIs available as part of the Services, then ProMobi reserves the right to place limits on access to such APIs (e.g., limits on numbers of calls or requests). Further, ProMobi may monitor Customer’s usage of such APIs and limit the number of calls or requests Customer may make if ProMobi believes that Customer’s usage is in breach of this Agreement or may negatively affect the Services (or otherwise impose liability on ProMobi).

2.9. Trial Subscriptions: If Customer receives free access or a trial or evaluation subscription to the Service (a “Trial Subscription”), then Customer may use the Services in accordance with the terms and conditions of this Agreement for a period of fourteen (14) days or such other period granted by ProMobi (the “Trial Period”). Trial Subscriptions are permitted solely for Customer’s use to determine whether to purchase a paid subscription to the Services. Trial Subscriptions may not include all functionality and features accessible as part of a paid Subscription Term. If Customer does not enter into a paid Subscription Term, this Agreement and Customer’s right to access and use the Services will terminate at the end of the Trial Period. ProMobi has the right to terminate a Trial Subscription at any time for any reason.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ProMobi WILL HAVE NO WARRANTY, INDEMNITY, SUPPORT, OR OTHER OBLIGATIONS WITH RESPECT TO TRIAL SUBSCRIPTIONS.

3. Customer Data

3.1. Rights in Customer Data: As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data as provided to ProMobi. Subject to the terms of this Agreement, Customer hereby grants to ProMobi a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data solely to the extent necessary to provide the Services to Customer.

3.2. Storage of Customer Data: ProMobi does not provide any long term archiving service. ProMobi agrees only that it will not intentionally delete any Customer Data from any Service prior to termination of Customer’s applicable Subscription Term. ProMobi expressly disclaims all other obligations with respect to storage.

3.3. Customer Obligations

a) *In General* Customer is solely responsible for the accuracy, content and legality of all Customer Data. Customer represents and warrants to ProMobi that Customer has all necessary rights, consents and permissions to collect, share and use all Customer Data as contemplated in this Agreement (including granting ProMobi the rights in Section 3.1 (Rights in Customer Data)) and that no Customer Data will violate or infringe (i) any third party intellectual property, publicity, privacy or other rights, (ii) any Laws, or (iii) any terms of service, privacy policies or other agreements governing the Customer Properties or Customer’s accounts with any Third-Party Platforms. Customer further represents and warrants that all Customer Data complies with the

AUP. Customer will be fully responsible for any Customer Data submitted to the Services by any Person as if it was submitted by Customer.

b) *No Sensitive Personal Information.* Customer specifically agrees not to use the Services to collect, store, process or transmit any Sensitive Personal Information. Customer acknowledges that ProMobi is not a Business Associate or subcontractor (as those terms are defined in HIPAA) or a payment card processor and that the Services are neither HIPAA nor PCI DSS compliant. ProMobi will have no liability under this Agreement for Sensitive Personal Information, notwithstanding anything to the contrary herein.

c) *Compliance with Laws.* Customer agrees to comply with all applicable Laws in its use of the Services. Without limiting the generality of the foregoing, Customer will not engage in any unsolicited advertising, marketing, or other activities using the Services, including without limitation any activities that violate the Telephone Consumer Protection Act of 1991, CAN-SPAM Act of 2003 or any other anti-spam laws and regulations.

3.4. Indemnification by Customer: Customer will indemnify, defend and hold harmless ProMobi from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with any claim arising from or relating to any Customer Data or breach or alleged breach by Customer of Section 3.3 (Customer Obligations). This indemnification obligation is subject to Customer receiving (i) prompt written notice of such claim (but in any event notice in sufficient time for Customer to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense, or settlement of such claim; and (iii) all necessary cooperation of ProMobi at Customer's expense. Notwithstanding the foregoing sentence, (a) ProMobi may participate in the defense of any claim by counsel of its own choosing, at its cost and expense and (b) Customer will not settle any claim without ProMobi's prior written consent, unless the settlement fully and unconditionally releases ProMobi and does not require ProMobi to pay any amount, take any action, or admit any liability.

3.5. Aggregated Anonymous Data: Notwithstanding anything to the contrary herein, Customer agrees that ProMobi may obtain and aggregate technical and other data about Customer's use of the Services that is non-personally identifiable with respect to Customer ("Aggregated Anonymous Data"), and ProMobi may use the Aggregated Anonymous Data to analyze, improve, support and operate the Services and otherwise for any business purpose during and after the term of this Agreement, including without limitation to generate industry benchmark or best practice guidance, recommendations or similar reports for distribution to and consumption by Customer and other ProMobi customers. For clarity, this Section 3.5 does not give ProMobi the right to identify Customer as the source of any Aggregated Anonymous Data.

4. Security

ProMobi agrees to use commercially reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of any Service or Customer Data. However, ProMobi will have no responsibility for errors in transmission, unauthorized third-party access or other causes beyond ProMobi's control. Visit ProMobi's [security practices](#) here.

5. Third-Party Platform Integrations

The Services may support integrations with certain Third-Party Platforms. In order for the Services to communicate with such Third-Party Platforms, Customer may be required to input credentials in order for the Services to access and receive relevant information from such Third-Party Platforms. By enabling use of the Services with any Third-Party Platform, Customer authorizes ProMobi to access Customer's accounts with such Third-Party Platform for the purposes described in this Agreement. Customer is solely responsible for complying with any relevant terms and conditions of the Third-Party Platforms and maintaining appropriate accounts in good standing with the providers of the Third-Party Platforms. Customer acknowledges and agrees that ProMobi has no responsibility or liability for any Third-Party Platform or any Customer Data exported to a Third-Party Platform. ProMobi does not guarantee that the Services will maintain integrations with any Third-Party Platform and ProMobi may disable integrations of the Services with any Third-Party Platform at any time with or without notice to Customer. For clarity, this Agreement governs Customer's use of and access to the Services, even if accessed through an integration with a Third-Party Platform.

6. Ownership

6.1. **Scalefusion Technology_**: This is a subscription agreement for access to and use of the Services. Customer acknowledges that it is obtaining only a limited right to the Services and that irrespective of any use of the words "purchase", "sale" or like terms in this Agreement no ownership rights are being conveyed to Customer under this Agreement. Customer agrees that ProMobi or its suppliers retain all right, title and interest (including all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the Services and all Documentation, professional services deliverables and any and all related and underlying technology and documentation and any derivative works, modifications or improvements of any of the foregoing, including as may incorporate Feedback (collectively, "**Scalefusion Technology**"). Except as expressly set forth in this Agreement, no rights in any **Scalefusion Technology** are granted to Customer. Further, Customer acknowledges that the Services are offered as an on-line, hosted solution, and that Customer has no right to obtain a copy of any of the Services, except for ProMobi Code and the ProMobi Apps in the format provided by ProMobi.

6.2. **Feedback**. Customer, from time to time, may submit Feedback to ProMobi. ProMobi may freely use or exploit Feedback in connection with any of its products or services.

7. Subscription Term, Fees & Payment

7.1. **Subscription Term and Renewals**: Unless otherwise specified on the applicable purchase order, each Subscription Term will have to be renewed explicitly, you will receive an email notification about the expiry of your Subscription Term at least thirty (30) days prior to expiration of the then-current Subscription Term.

7.2. **Fees and Payment**: All fees are as set forth in the applicable purchase order and will be paid by Customer within thirty (30) days of invoice, unless (a) Customer is paying via Credit Card (as defined below) or (b) otherwise specified in the applicable purchase order. Except as expressly set forth in Section 9 (Limited Warranty) and Section 14 (Indemnification), all fees are non-refundable. The rates in the purchase

order and/or invoices are valid for the initial twelve (12) month period of each Subscription Term and thereafter may be subject to an automatic adjustment increase of up to ten percent (10%) per year. Customer is responsible for paying all Taxes, and all Taxes are excluded from any fees set forth in the applicable purchase order. If Customer is required by Law to withhold any Taxes from Customer's payment, the fees payable by Customer will be increased as necessary so that after making any required withholdings, ProMobi receives and retains (free from any liability for payment of Taxes) an amount equal to the amount it would have received had no such withholdings been made. Any late payments will be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less.

7.3. Payment Via Credit Card: If you are purchasing the Services via credit card, debit card or other payment card ("Credit Card"), the following terms apply:

- *Foreign Transaction Fees.* Customer acknowledges that for certain Credit Cards, the issuer of Customer's Credit Card may charge a foreign transaction fee or other charges.
- *Invalid Payment:* If a payment is not successfully settled due to expiration of a Credit Card, insufficient funds, or otherwise, Customer remains responsible for any amounts not remitted to ProMobi and ProMobi may, in its sole discretion, either (i) invoice Customer directly for the deficient amount, or (ii) terminate the Subscription Term as well as this Agreement.
- *Payment of Outstanding Fees.* Upon any termination or expiration of the Subscription Term, ProMobi will invoice Customer directly for any outstanding fees for Customer's use of the Services during the Subscription Term, after which ProMobi will not charge for any additional fees, once the outstanding amount is paid in full.

7.4. Suspension of Service. If Customer's account is thirty (30) days or more overdue, in addition to any of its other rights or remedies (including but not limited to any termination rights set forth herein), ProMobi reserves the right to suspend Customer's access to the applicable Service (and any related services) without liability to Customer until such amounts are paid in full. ProMobi also reserves the right to suspend Customer's access to the Services without liability to Customer if Customer's use of the Services is in violation of the AUP.

7.5. Subscription Downgrade. Customer cannot downgrade their plan in the middle of an existing active subscription. However, customers can downgrade their plan at the renewal of their existing subscription. The newly chosen plan will be effective only after the renewal. Customers can choose to downgrade to the then-available subscription plan while renewal.

7.6. Subscription Plan. ProMobi reserves the right to change its offering of subscription plans, including by limiting or ceasing to offer any subscription plans, including any associated features as well, upon sending a written notice to Customer, which may be by email. Subscription plans may not be available to all customers and regions.

8. Term and Termination

8.1. Term. This Agreement is effective as of the Effective Date and expires on the date of expiration or termination of all Subscription Terms.

8.2. Termination for Cause. Either party may terminate this Agreement (including all related purchase orders) if the other party (a) fails to cure any material breach of this Agreement (including a failure to pay fees) within thirty (30) days after written notice; (b) ceases operation without a successor; or © seeks protection under any bankruptcy, receivership, trust deed, creditors' arrangement, composition, or comparable proceeding, or if any such proceeding is instituted against that party (and not dismissed within sixty (60) days thereafter).

8.3. Effect of Termination. Upon any expiration or termination of this Agreement, Customer will immediately cease any and all use of and access to all Services (including any and all related Scalefusion Technology) and delete (or, at ProMobi's request, return) any and all copies of the Documentation, any Scalefusion passwords or access codes and any other ProMobi Confidential Information in its possession. Provided this Agreement was not terminated for Customer's breach, Customer may retain and use internally copies of all reports exported from any Service prior to termination. Customer acknowledges that following termination it will have no further access to any Customer Data input into any Service, and that ProMobi may delete any such data as may have been stored by ProMobi at any time. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law or otherwise.

8.4. Survival. The following Sections will survive any expiration or termination of this Agreement: 2.7 (General Restrictions), 2.9 (Trial Subscriptions), 3.2 (Storage of Customer Data), 3.4 (Indemnification by Customer), 3.5 (Aggregated Anonymous Data), 6 (Ownership), 7.2 (Fees and Payment), 7.3 (Payment Via Credit Card), 8 (Term and Termination), 9.2 (Warranty Disclaimer), 12 (Limitation of Remedies and Damages), 13 (Indemnification), 14 (Confidential Information) and 16 (General Terms).

9. Limited Warranty

9.1. Limited Warranty: ProMobi warrants, for Customer's benefit only, that each Service will operate in substantial conformity with the applicable Documentation. ProMobi's sole liability (and Customer's sole and exclusive remedy) for any breach of this warranty will be, at no charge to Customer, for ProMobi to use commercially reasonable efforts to correct the reported non-conformity, or if ProMobi determines such remedy to be impracticable, either party may terminate the applicable Subscription Term and Customer will receive as its sole remedy a refund of any fees Customer has pre-paid for use of such Service for the terminated portion of the applicable Subscription Term. The limited warranty set forth in this Section 9.1 will not apply: (i) unless Customer makes a claim within thirty (30) days of the date on which Customer first noticed the non-conformity, (ii) if the error was caused by misuse, unauthorized modifications or third-party hardware, software or services, or (iii) to use provided on a no-charge, trial or evaluation basis.

9.2. Warranty Disclaimer: EXCEPT FOR THE LIMITED WARRANTY IN SECTION 9.1, ALL Services and PROFESSIONAL SERVICES ARE PROVIDED "AS IS". NEITHER PROMOBI NOR ITS SUPPLIERS MAKES ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. ProMobi does not warrant that Customer's use of THE Services will be uninterrupted or error-free, nor does ProMobi

warrant that it will review the Customer Data for accuracy or that it will preserve or maintain the Customer Data without loss OR CORRUPTION. PROMOBI SHALL NOT BE LIABLE FOR THE RESULTS OF ANY COMMUNICATIONS SENT OR ANY COMMUNICATIONS THAT WERE FAILED TO BE SENT USING THE SERVICES. ProMobi SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES OR OTHER PROBLEMS INHERENT IN USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS, THIRD-PARTY PLATFORMS OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF ProMobi. CUSTOMER MAY HAVE OTHER STATUTORY RIGHTS, BUT THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE SHORTEST PERIOD PERMITTED BY LAW.

10. Support

During the Subscription Term of each Service, ProMobi will provide end user support in accordance with ProMobi's [Support Policy](#) ("Support Policy").

11. Professional Services

ProMobi may provide the professional consulting services ("Professional Services") purchased in the applicable purchase order. The scope of Professional Services will be as set forth in a Statement of Work ("SOW") referencing this Agreement and executed by both parties describing the work to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information ("SOW"). Unless Professional Services are provided on a fixed-fee basis, Customer will pay ProMobi at the per-hour rates set forth in the Purchase Order Form (or, if not specified, at ProMobi's then-standard rates) for any excess services. Customer will reimburse ProMobi for reasonable travel and lodging expenses as incurred. Customer may use anything delivered as part of the Professional Services in support of authorized use of the Services and subject to the terms regarding Customer's rights to use the Service set forth in Section 2 (ProMobi Services) and the applicable SOW, but ProMobi will retain all right, title and interest in and to any such work product, code or deliverables and any derivative, enhancement or modification thereof created by ProMobi (or its agents).

12. Limitation of Remedies and Damages

12.1. *Consequential Damages Waiver.* EXCEPT FOR EXCLUDED CLAIMS (DEFINED BELOW), NEITHER PARTY (NOR ITS SUPPLIERS) SHALL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOSS OF USE, LOST DATA, LOST PROFITS, FAILURE OF SECURITY MECHANISMS, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12.2. *Liability Cap.* PROMOBI'S AND ITS SUPPLIERS' ENTIRE LIABILITY TO CUSTOMER ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY CUSTOMER TO PROMOBI DURING THE PRIOR TWELVE (12) MONTHS UNDER THIS AGREEMENT.

12.3. *Excluded Claims.* "Excluded Claims" means any claim arising (a) from Customer's breach of Section 2.7 (General Restrictions); (b) under Section 3.3 (Customer Obligations) or 3.4 (Indemnification by Customer); or © from a party's

breach of its obligations in Section 15 (Confidential Information) (but excluding claims arising from operation or non-operation of any Service).

12.4. Nature of Claims and Failure of Essential Purpose. The parties agree that the waivers and limitations specified in this Section 13 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy specified in this Agreement is found to have failed of its essential purpose.

13. Indemnification

ProMobi will defend Customer from and against any claim by a third party alleging that a Service when used as authorized under this Agreement infringes a U.S. patent, U.S. copyright, or U.S. trademark and will indemnify and hold harmless Customer from and against any damages and costs finally awarded against Customer or agreed in settlement by ProMobi (including reasonable attorneys' fees) resulting from such claim, provided that ProMobi will have received from Customer: (i) prompt written notice of such claim (but in any event notice in sufficient time for ProMobi to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense and settlement (if applicable) of such claim; and (iii) all reasonable necessary cooperation of Customer. If Customer's use of a Service is (or in ProMobi's opinion is likely to be) enjoined, if required by settlement or if ProMobi determines such actions are reasonably necessary to avoid material liability, ProMobi may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for Customer the right to continue using such Service; or if (a) and (b) are not commercially reasonable, © terminate this Agreement and refund to Customer the fees paid by Customer for the portion of the Subscription Term that was paid by Customer but not rendered by ProMobi. The foregoing indemnification obligation of ProMobi will not apply: (1) if such Service is modified by any party other than ProMobi, but solely to the extent the alleged infringement is caused by such modification; (2) if such Service is combined with products or processes not provided by ProMobi, but solely to the extent the alleged infringement is caused by such combination; (3) to any unauthorized use of such Service; (4) to any action arising as a result of Customer Data or any third-party deliverables or components contained within such Service; (5) to the extent the alleged infringement is not caused by the particular technology or implementation of the Service but instead by features common to any similar product or service; or (6) if Customer settles or makes any admissions with respect to a claim without ProMobi's prior written consent. THIS SECTION 13 SETS FORTH ProMobi's AND ITS SUPPLIERS' SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

14. Confidential Information

Each party (as "**Receiving Party**") agrees that all code, inventions, know-how, business, technical and financial information it obtains from the disclosing party ("**Disclosing Party**") constitute the confidential property of the Disclosing Party ("**Confidential Information**"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be confidential or proprietary due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any Scalefusion Technology, performance information relating to any Service, and the terms and conditions of this Agreement will be deemed Confidential Information of ProMobi without any marking or further

designation. Except as expressly authorized herein, the Receiving Party will (1) hold in confidence and not disclose any Confidential Information to third parties and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement. The Receiving Party may disclose Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know (including, for ProMobi, the subcontractors referenced in Section 17.8 (Subcontractors)), provided that such representatives are bound to confidentiality obligations no less protective of the Disclosing Party than this Section 14 and that the Receiving Party remains responsible for compliance by any such representative with the terms of this Section 14. The Receiving Party's confidentiality obligations will not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information. The Receiving Party may make disclosures to the extent required by law or court order, provided the Receiving Party notifies the Disclosing Party in advance and cooperates in any effort to obtain confidential treatment. The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

15. Co-Marketing

At the request of ProMobi, Customer may agree to participate in other reasonable marketing activities that promote the benefits of the Services to other potential customers and to use of Customer's name and logo on ProMobi's web site and in ProMobi promotional materials. Customer agrees that ProMobi may disclose Customer as a customer of ProMobi.

16. General Terms

16.1. Assignment: This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in connection with a merger, reorganization, acquisition or other transfer of all or substantially all of such party's assets or voting securities. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section 16.1 will be null and void.

16.2. Severability: If any provision of this Agreement will be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect.

16.3. Entire Agreement: This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement. Customer acknowledges that the Services are on-line, subscription-based products, and that in order to provide improved customer experience ProMobi

may make changes to the Services, and ProMobi will update the applicable Documentation accordingly. The support terms described in the Support Policy may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices (but the modifications will not materially decrease ProMobi's obligations as compared to those reflected in such terms as of the Effective Date).

16.4. Force Majeure: Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events that occur after the signing of this Agreement and that are beyond the reasonable control of such party, such as a strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or telecommunications or data networks or services, or refusal of a license by a government agency.

16.5. Subcontractors: ProMobi may use the services of subcontractors and permit them to exercise the rights granted to ProMobi in order to provide the Services under this Agreement, provided that ProMobi remains responsible for (i) compliance of any such subcontractor with the terms of this Agreement and (ii) for the overall performance of the Services as required under this Agreement.

16.6. Subpoenas: Nothing in this Agreement prevents ProMobi from disclosing Customer Data to the extent required by law, subpoenas, or court orders, but ProMobi will use commercially reasonable efforts to notify Customer where permitted to do so.

16.7 Changes to this Agreement. We may update or modify this Agreement from time to time, including any referenced policies and other documents. If a revision meaningfully reduces your rights, we will use reasonable efforts to notify you (by, for example, sending an email to the billing or technical contact you designate in the applicable purchase Order, posting on our blog, through your ProMobi account, or in the Product itself). If we modify the Agreement during your License Term or Subscription Term, the modified version will be effective upon your next renewal of a License Term, Support and Maintenance term, or Subscription Term, as applicable. In this case, if you object to the updated Agreement, as your exclusive remedy, you may choose not to renew, including cancelling any terms set to auto-renew. With respect to No-Charge Products, accepting the updated Agreement is required for you to continue using the No-Charge Products. You may be required to click through the updated Agreement to show your acceptance. If you do not agree to the updated Agreement after it becomes effective, you will no longer have a right to use No-Charge Products. For the avoidance of doubt, any purchase Order is subject to the version of the Agreement in effect at the time of the Order.

16.8. Counterparts: This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

ACCELERATING BUSINESS WITH SPOORS – EFFORT FIELD SERVICE MANAGEMENT IN THE CLOUD

If your business need advance functionalities for managing Service orders, Dispatching technicians, Work planning, Route optimization Effort is the product. Built for the cloud, Effort Field Service Management has enabled staff to work on the go, helping the highest performing service organizations tackle a new generation of field service challenges.

Cloud solutions to field service management means there's no infrastructure to manage, making it easy to provision new operations, upscale or add more functionalities as soon as you need it.

Cloud-based solutions are very attractive for field service because they may be more flexible, readily extensible and more accessible being cost effective.



High on Configurability

The advantages of using effort is the enhanced operational flexibility and agility it gives your business. Our cloud services support options for configuration, customization & integrations and it provides the choice of when to deploy updates, except for mandatory essential patches.

Unique Value proposition

1. Dynamic Mobile **Form engine**
2. **Offline Mobile App** for IOS & Android Devices
3. Flexibility to Capture Images, Videos, Audio
4. **Geotagging** of Activities



GENERAL TERMS AND CONDITION

- Signup/registration on the Website/App is available only to the person who can form legally binding contracts under Indian Contract Act, 1872. Persons who are "incompetent to contract" within the meaning of the Indian Contract Act, 1872 including minors, un-discharged insolvents etc. are not eligible to register on the Website/App. As a minor if User wish to use the Website/App, shall be registered by legal guardian or parents on the Website/App. If it comes to the knowledge of Spoors Private Limited that the User registered on the Website/App via providing the personal information is under the age of 18 years, shall be removed from the Website/App by Spoors Private Limited. Spoors Private Limited reserves the right to terminate the membership and / or refuse to provide the User with access to the Website/App if it is brought to Spoors Private Limited notice or if it is discovered that the signup/registration over the Website/App is done by a User, under the age of 18 years.
- Signup/registration of the User on the Website/App is necessary to access the Website/App and use the services. User shall be required to signup/register for an account on the Website/App by providing email address, name, password and user name. User shall provide accurate, complete and updated information in order to signup/register on the Website/App to use the services.
- User represent, warrant, and agree that User shall not use the services in a manner that:
 1. Infringes or violates the intellectual property rights or any other rights of anyone else.
 2. Violates any law or regulation;
 3. Is harmful, fraudulent, deceptive, threatening, harassing, defamatory, obscene, or otherwise objectionable;

4. Attempts, in any manner, to obtain the password, account, or other security information from any other User;
 5. Violates the security of any computer network, or cracks any passwords, or security encryption codes;
- User accepts the Website/App Terms and condition, Privacy Policy by using the “OTP” to signup/register when registering and logging into the Website/App to use the services.
 - Spoors Private Limited might change the methodology or functionality of the Website/App at any point of time and intimation to that extent shall be mentioned in the Website/App under Terms and Conditions.
 - Spoors Private Limited shall always try to improve the services provided by the Website/App which shall include suspension or discontinuation of any part of the services. Spoors Private Limited shall introduce features or impose limit on certain features or restrict access to parts or all of the services provided through the Website/App. A notification of any such action shall be sent to the User in advance.
 - Spoors Private Limited reserves the right to remove any content provided on the Website/App at any time without any reason or any notice of any such action by Spoors Private Limited on the Website/App. Subject to the terms and conditions set forth in this Agreement. Spoors Private Limited grants User a non-exclusive, non-transferable, limited right to access and use this Website/App and the information thereon. User agrees not to interrupt or attempt to interrupt the services of the Website/App in any way.
 - The information provided on the Website/App are in relation to providing services such as text, graphics, article, photos, images are protected by the Copyright and other Intellectual Property Laws. User promises to abide by all Copyright notices, Trademark rules and the User won't use, copy, reproduce, modify, translate, publish, broadcast, transmit, distribute, perform, upload, display, license, sell or otherwise exploit for any purpose any Content not owned by the User without the prior written consent of Spoors Private Limited. User won't modify, publish, transmit, participate in the transfer or sale

of, reproduce, create derivative works based on, or otherwise exploit any of the Services.

- The information on this Website/App has been included in good faith and is for general purposes only. It should not be relied upon for any specific purpose and no representation or warranty is given as regards its accuracy or completeness.
- No reproduction of any part of the Website/App may be sold or distributed for commercial gain, nor shall it be modified or incorporated in any other work, publication or site, whether in hard copy or electronic format, including postings to any other site. Spoors Private Limited reserves all other rights.
- Neither Spoors Sons and Spoors affiliates, nor their affiliates' officers, employees or agents shall be liable for any loss, damage or expense arising out of any access to or use of this Website/App including without limitation, any loss of profit, indirect, incidental or consequential loss.
- In relation to any circumstances that arise due to the Use of the Website/App shall be communicated to the customer care of the Website/App. User understands that there may be instances of difficulty in accessing or receiving email communication. We are not responsible if any email notice gets caught by User's SPAM folder, or if User do not see the email, or if User has given us an incorrect email id or if for any other reason You do not receive the email notice. Therefore, we encourage User to frequently open the Application to monitor any changes. User continued use of or access to the Services following the posting of any changes to this Agreement constitutes acceptance of those changes.
- Any failure of functioning of the Website/App shall be intimated by the User to Spoors Private Limited and Spoors Private Limited shall duly try to resolve the issue. Spoors Private Limited shall not be liable for any kind of damages or losses faced by the User due to functionality of the Website/App.

- Payment of such services shall be in accordance to the charges available on the app store during purchase of such services, or as informed by Spoors Private Limited to the User based on the services availed.
- Spoors Private Limited will protect the data to the extent required by applicable law, and subject to applicable law, Spoors Private Limited will take every security measure for protection of the data provided. Spoors Private Limited will not disclose any information to any third-party and will not engage directly with another processor to provide the Services to the User. Spoors Private Limited will keep records of its processing activities with respect to any data and cooperate with authorized person in respect of any complaint or investigation relating to such data. Website/App will notify the User in respect of any suspected or actual breach of data security or other unauthorized access or processing of any such data .
- User agrees to indemnify and hold Spoors Private Limited, its affiliates, officers, agents, employees, and partners harmless for and against any and all claims, liabilities, damages (actual and consequential), losses and expenses (including attorneys' fees) arising from or in any way related to any third party claims relating to (a) User's use of the Services (including any actions taken by a third party using User account), and (b) User's violation of these Terms. In the event of such a claim, suit, or action, Spoors Private Limited shall provide notice of the claim to the contact information provided by the User during signup/registration on the Website/App. Failure to deliver such notice shall not eliminate or reduce User's indemnification obligations hereunder.
- Spoors Private Limited shall own all rights, title, and interest in the feedback provided by the User and Spoors Private Limited shall be entitled to use the feedback without restriction, even if the User has indicated such feedback as confidential or restricted for improvement of Website/App services. Website/App shall not be under any obligation of confidentiality, express or implied, with respect to the feedback. Spoors Private Limited shall be entitled to use or disclose any such feedback for any purpose, in any

way required and Spoors Private Limited will not be liable for any compensation for any such disclosure under any circumstances.

- Spoors Private Limited will suspend the Users right to use the services immediately upon notice of any security risk due to the Users use of the services which may impact the App or other systems or if it comes to the knowledge of any fraudulent use of Website/App.
- This Agreement is the complete and exclusive statement of the agreements between User and Spoors Private Limited with respect to the subject matter hereof and supersedes all other communications or representations or agreements (whether oral, written or otherwise) relating thereto.
- The failure of either party at any time to require performance of any provision of this Agreement in no manner shall affect such party's right at a later time to enforce the same. No waiver by either party of any breach of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be, or construed as, a further or continuing waiver of any other such breach, or a waiver of any other breach of this Agreement.
- If any provision of this Agreement shall to any extent be held invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions of this Agreement shall in no way be affected or impaired thereby and each such provision of this Agreement shall be valid and enforceable to the fullest extent permitted by law. In such case, this Agreement shall be reformed to the minimum extent necessary to correct any invalidity, illegality or unenforceability, while preserving to the maximum extent the rights and commercial expectations of the parties hereto, as expressed herein.
- These Terms are governed by and will be construed under the laws of India, without regard to the conflicts of laws provisions thereof, unless prohibited by law. Any dispute arising from or relating to the subject matter of these Terms shall be finally settled in

Hyderabad, India. THIS CLAUSE SHALL SURVIVE THE TERMINATION OR EXPIRY OF THIS AGREEMENT.

- **I AGREE TO THE ABOVE TERMS AND CONDITIONS**

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh
Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)
Subcategory N: Secure LAN Access

Client Company name:	WEC Energy Group
Client name of contact:	Steve Liegl
Client contact title:	Director Infrastructure and Operations
Client is a daily user, occasional user, etc.:	Daily User

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to James Rose no later than Friday, November 6th.

Thank you for your assistance in this process.

- 1. For what services do you use USCC's product, and how long have you been USCC's customer?**
We currently use USCC for voice and data services across our field crew members. These crew members provide support to our electric and gas distribution system. Customer since 1988.

- 2. Would you recommend USCC to other customers? Why?**
Yes, the attention that our account team has on the account and their ability to provide services directly related to our needs saves a lot of time. In addition, coverage and network quality has been key attributes supporting our desire to put our wireless voice and data needs on the USCC network.

- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

USCC has provided timely response to the effort needed to establish a private VPN within our environment. This created an easy to use solution for our end users.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

We have not had to file any complaints, nor have we had any major disruptions impacting our business in recent years.

- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

All voice and data products continue to meet our business needs through their reliability and expansive wireless service. The expansion of service in Wisconsin has been a great benefit to our mobile users as well.

- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

Nothing at this time.

- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

Nothing at this time

- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

All products have been described. We have business with competing wireless carriers, and I would say that our needs are met with the USCC account team and network capabilities.

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory A: Fleet Management

Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)

Client Company name:

Knoxville-Knox County Head Start

Client name of contact:

Lisa Silverman & Jodie Fain

Client contact title:

Data Integration Manager & Program Manager

Client is a daily user, occasional user, etc.:

Administrators Daily User

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Jim Cosmos no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

- Customer with USC for 15 or more years
- Cellular phones (iPhones), tablets with data (LG G5 & Samsung Galaxy Tab A), Ready Fleet Vehicle Monitoring & IBM Maas 360

2. Would you recommend USCC to other customers? Why? YES

- Always responsive to our needs
- Have a yearly meeting to discuss our current service and rates
- USCC has made recommendations about things we need to do to lower our bill
- USCC monitors the data usage and will make suggestions regarding plans
- USCC has helped KKCHS to meet several needs of the program
- KKCHS wanted smart phones for all classrooms however, we could not afford the monthly data plans. USCC created a plan where all classrooms could have a smart phone without data. The phone is able to connect to Wi-Fi at each location and the smart phone can be used. This is at a much lower cost than a data plan for each smart phone.
- USCC was able to work out the purchasing of tablet cases for each of the tablets.

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

- In the beginning of the IBM Maas 360, USCC had at least 3 meetings with KKCHS, USCC and IBM on the installation of the program.
- With the purchase of an initial 400 tablets, USCC enrolled all tablets in the program.
- The additional delivery of our purchase of 200 tablets was timely and USCC assisted with the installation of the IBM Maas360, as well as providing written instructions to install, update and reset IBM Maas360 on the tablets.
- USCC delivered all tablets in the time frame that was initially presented.

4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?

- USCC has always been extremely customer service oriented.
- USCC responds very quickly to emails, texts, and calls.
- USCC will come on site and work to help implement new devices and software.

5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?

- Yes, the IBM Maas360 worked the way USCC initially presented it to KKCHS.
- It has met the expectations of KKCHS.

6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?

- The relationship with USCC has been superb as it has been in the past.

- One thing that we wish we had was a clearer understanding of how the IBM Maas360 was going to work for our KKCHS end user (Head Start / Early Head Start Parents).

7. Is there anything else you think we should know about working with USCC or using USCC's products and services?

- USCC has been extremely responsive and supportive to the inquiries and needs of KKCHS.

8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?

- iPhones (in excess of 100)
- Tablets (LG G 5 – 670)
- Tablets (Samsung Galaxy Tab A --- 65)
- Ready Fleet Monitoring Units (44)
- IBM Maas360 (600)
- KKCHS does not have any other relationships with USCC other than what is listed above.

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh
Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)

Client Company name:	Horizon Home Care and Hospice, Inc.
Client name of contact:	Randy Rybakowicz
Client contact title:	Director, Information Technology
Client is a daily user, occasional user, etc.:	Daily

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to James Rose no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

We are long time (10 years+) customers and consider USCC a strategic partner. For the majority of that time, we have utilized their mobile hardware and cellular services. A few years ago, we wanted to improve the management of our fleet. USCC introduced Apple DEP and IBM MaaS360 to help us streamline onboarding and ongoing management and security of a growing fleet.

2. Would you recommend USCC to other customers? Why?

USCC is definitely recommended. USCC has been a critical "partner" for many years for supplying the hardware and communication services our business relies on. Beyond being a provider in a highly competitive space, they recognize the nature of our business and go the

extra step in helping where ever possible to provide white-glove service. USCC understands customer commitment and works hard to be part of the future possibilities for us.

- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services?**

2020 introduced a myriad of challenges due to the Pandemic. UScellular was dynamic during the unusual conditions and coordinated our service and hardware migration through remote teams and tools. Despite the recognized obstacles, this was the smoothest transition we have experienced thanks to their cooperative planning; including fully utilizing DEP and MaaS360 to efficiently complete the initiative.
- 4. How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

Reiterating, the Pandemic created many obstacles from supply chain to project logistics. USCC was fully responsive to ensure we could fulfil the order, while staying true to our desired timeline.
- 5. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

USCC is a terrific partner and exceeded our expectations transitioning a significant fleet of phones and accounts. Anomalies were handled quickly and efficiently. No major hurdles were experienced. Our associates were delighted with their new devices, quality of service and the process of receiving them.
- 6. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

We transitioned from aging mobile technology to the latest available. No complaints, associates are impressed with the entire experience and performance of the process, service and devices.
- 7. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

In all honesty, USCC stepped up, partnered up, provided exactly what we needed, when we needed it and extremely competitively. USCC is also invested in what we do and how we serve the community. Fully supporting us where it counts to provide unique community services.
- 8. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

We operate in Wisconsin, primarily in the Greater Milwaukee area. The service is very good and continues to improve. The service we use is integral to our business and the lives of our patients. Anything less than optimal would not be acceptable.
- 9. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

As part of the USCC family, we were introduced to Apple DEP and IBM MaaS360. The utilization of these tools enabled us to remove at least 30 minutes per device deployment. Automation, centralization and standardizing customer experience have been crucial as we operate with an extremely lean support team.

Appendix M

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory D, E, and F: Field Service Management, Workforce Management, and Mobile Data Collection / Mobile Forms

Effort +



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
Effort+ - An acronym that stands for "Effortless Field Force Optimization and Reporting Tool"
- b. General Application Area
Subcategories D, E, and F
- c. General capabilities provided
Capabilities include:
 - Dynamic Mobile Form engine, to define and capture data.
 - Offline Mobile data collection App for IOS & Android.
 - Flexibility to Capture different data types such as images, videos, and audio along with signature.
 - Geotagging of activities to ensure activities were performed on-premise.
 - Route optimization to ensure maximum coverage.
 - Workflow automation to take care of approvals and exceptions, that allow for data to flow to necessary people for action (all through mobile apps).
- d. Expected impact on cost/performance/functionality, etc.
 - World over FSM and Workforce management has been a key challenge and organizations have deployed solutions that are heavy and expensive.
 - Effort+ ensures that the deployment is hassle-free, economical and scalable all through a cloud-based platform, secure storage and dynamic mobile application.
 - Experience and studies have proven that cost savings of minimum 35% is achieved when organizations choose to deploy Effort+.
- e. Subcontractors/partners involved in delivering service
Goldie Group is a regional partner with Spoors the brand owner of Effort+. We will be serving and servicing the Workforce, FSM and Mobile data collection needs of the client along with Spoors team.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described

Our tool provides:

- A dynamic form builder with 30+ data types that allows for quickly building and deploying mobile forms that can be used by field personnel to both record and collect data.
- Flexible and easy workflows that allow for approvals and sanctions on the fly with managers and subordinates working their way through the mobile app that serves them the necessary data.
- Cloud-based service - no worry on infrastructure downtime or scalability.
- Offline data collection along with Geo-stamps ensure veracity of data!
- Ability to create 1000s of forms on the go using a dynamic dashboard that also serves as a single window to provide comprehensive views of activities and data flow.

- b. Applicability to government needs

The solution is dynamic and domain-agnostic. Hence can be applied to any governmental needs. In fact, some of the local government in Indian region have used it to collect data of farmers, distribution of subsidies, etc.

Caters to all the governmental protocols and procedures ensuring data privacy and security.

- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.

Provide references

500+ global customers from various domains including Siemens, AtoS Switzerland, HomeCredit, Truemoney, L&T and other big names.

- d. Overall interoperability of turnkey system for government use

The solution is a data definition and collection tool. Works with a simple database that allows for data to flow to different systems through custom APIs.

- e. Accessories available for turnkey offering

N/A

- f. Thoroughness of the vetting process used to select partners

Goldie Group selects and offers solutions that are robust and proven in the market. We work to ensure our 30-year legacy is not compromised.

- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

Client partners usually do integration tests as appropriate to suit their needs.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
 - Goldie Group and Spoors team will work towards initial form and workflow development as needed.
 - Will ensure that sanity and acceptance is done for forms and work flow deployments.
 - A Business Analysts will be available long-term for consultation at cost (USD \$75 per man hour).
- b. Project coordination
 - Goldie group will project manage all the operations and deliverables with all the involved parties and the client partners.
- c. Installation and Testing process
 - Initial form definitions, creation and deployment will be done by Goldie Group.
 - Field tests can be done in conjunction with client teams along with Goldie Group's involvement.
 - Once the acceptance is signed off mass roll out will be ensured by Goldie Group team to the necessary devices/personnel.
- d. Client Infrastructure and support assessment process
 - Our systems are all cloud-based and assessment if need be can be performed by the client partners.
 - We do regular security audits to ensure there is no data leakage or security breach (with third party assessments both for platform and the mobile applications). PEN (Penetration) tests are performed for checking security breaches, on a periodic basis.
- e. End user Acceptance process
 - Goldie will work with client partner to define the final acceptance document.
 - Goldie will work with client teams to sign-off on all of the agreed terms before mass roll out.
- f. Approach to maintenance and support
 - Cloud-based systems are generally taken care of by Goldie's partners and hence uptime and availability are ensured to 99.99% basis cloud service providers.
 - SLAs and insurances can be provided as a separate document should there be a need.
- g. Initial and Ongoing Training provided
 - Initial hand holding will be done, and device deployments will be assisted.
 - Ongoing training for new features are conducted on a regular basis.
 - Ongoing support can be purchased, and our BA (Business Analysts) will work remotely or on-prem to hand hold the teams. Incidentals, travel, boarding during on-prem visits will be borne by the clients.
- h. On-going support and enhancement over the life of the agreement
 - Free updates and feature inclusions are covered as part of the license agreement.
 - Support is included in the licensing cost. On-prem support is chargeable.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
Separate document on SLAs will be shared on a need basis once we are onboard with client partners. This shall detail availability, uptime, and other insurance measures to ensure smooth business operations.
- b. Experience and qualifications of partners and subcontractors
Goldie Group celebrates a 30+ year experience and knowhow in operations, warehousing, distribution and servicing technology needs for clients. Spoors is a young and dynamic solution company with more than 8 years of experience and several man years of technical know-how. The dynamic duo shall ensure our clients succeed even during tough times like the current pandemic.
- c. Description of Additional Integration and Consulting Services provided
 - On a need basis Goldie Group shall develop custom software and solutions that are required to augment the current business operations of the client
 - Our current supply chain platforms and back end integrations will also come in use for the large-scale deployment in disparate geographies.

Scalefusion MDM: Unified Device & Endpoint Management Solution

Terms of Service

Version: 4.0

Effective Date: 1 February, 2020

This “**Scalefusion (formerly MobiLock Pro)**” Terms of Service Agreement (the “Agreement”) is between you and ProMobi Technologies Pvt Ltd (India - U74900PN2014PTC150210) (“ProMobi”). If you are agreeing to this Agreement not as an individual but on behalf of your company, then “Customer” or “you” means your company, and you are binding your company to this Agreement. ProMobi may modify this Agreement from time to time, subject to the terms in Section 16.7 (Changes to this Agreement) below.

By clicking on the “I agree” (or similar button/link/checkbox) that is presented to you at the time of your Order, or by using or accessing ProMobi products, you indicate your assent to be bound by this Agreement.

Scope of the Agreement: This Agreement governs your initial purchase as well as any future purchases made by you that reference this Agreement. This Agreement includes our [Privacy Policy](#), our [Acceptable Use Policy](#), any Orders, and any other referenced policies and attachments. This Agreement applies to Scalefusion add-ons or plugins that you purchase from the Scalefusion website or from authorised resellers and distributors. However, it does not apply to apps, add-ons or plugins from other vendors that you install on your managed devices.

The “**Effective Date**” of this Agreement is the date which is the earlier of (a) Customer’s initial access to any Service (as defined below) through any online provisioning, registration or order process or (b) the effective date of the first Order Form referencing this Agreement.

As used in this Agreement, “ProMobi” means (a) ProMobi Technologies Pvt. Ltd., an Indian corporation with registered office at 303, Welworth Classic PLNo:2+3, SNo: 22/2, Wadgaonsheri, Pune, MH 411014, India.

ProMobi Products: This agreement governs (A) ProMobi’s software subscriptions to online software-as-a-service products

Account Registration

Revisions to this agreement: From time to time, ProMobi may modify this Agreement. Unless otherwise specified by ProMobi, changes to this term will be effective upon renewal of Customer’s current Subscription Term (as defined below) or entry into a new purchase order form. ProMobi will use reasonable effort to inform Customer of the changes through communications via Customer’s account, email or other means. In some cases Customer may be required to click to accept the new

terms or otherwise agree to the modified agreement before renewing the Subscription Term or entering into a new purchase order form, and in any event continued use of the ProMobi's products or services after the updated terms of this Agreement goes into effect will constitute Customer's acceptance of such updated terms. If ProMobi specifies that changes to the new terms will take effect prior to Customer's next renewal or purchase order (due to legal compliance or product change reasons) and Customer objects to such changes, Customer may terminate the applicable Subscription Term and receive as its sole remedy a refund of any fees Customer has pre-paid for use of the applicable Services for the terminated portion of the Subscription Term.

BY INDICATING YOUR ACCEPTANCE OF THIS AGREEMENT OR ACCESSING OR USING ANY SERVICES, YOU ARE AGREEING TO BE BOUND BY ALL TERMS, CONDITIONS, AND NOTICES CONTAINED OR REFERENCED IN THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, PLEASE DO NOT USE ANY SERVICES. FOR CLARITY, EACH PARTY EXPRESSLY AGREES THAT THIS AGREEMENT IS LEGALLY BINDING UPON IT. THIS AGREEMENT CONTAINS MANDATORY ARBITRATION PROVISIONS THAT REQUIRE THE USE OF ARBITRATION TO RESOLVE DISPUTES, RATHER THAN JURY TRIALS. PLEASE READ IT CAREFULLY.

1. Definitions

“Scalefusion (formerly MobiLock)” or “Scalefusion (formerly MobiLock Pro)” means a proprietary Enterprise Mobility Management solution developed, owned and marketed by ProMobi as software-as-a-service solution. In this agreement it will further be referred as **“Scalefusion”** only.

“Affiliate” means any entity under the control of Customer where “control” means ownership of or the right to control greater than 50% of the voting securities of such entity.

“AUP” means ProMobi's [Acceptable Use Policy](#).

“Contractor” means an independent contractor or consultant who is not a competitor of ProMobi.

“Customer Data” means any data of any type that is submitted to the Services by or on behalf of Customer, including without limitation: (a) data submitted, uploaded or imported to the Services by Customer (including from Third Party Platforms) and (b) data provided by or about People (including chat and message logs) that are collected from the Customer use of the Services.

“Customer Properties” means Customer's devices, apps, files owned and operated by (or for the benefit of) Customer through which Customer uses the Services to manage their account and devices.

“Dashboard” means Scalefusion's user interface for accessing and administering the Services that Customer may access via the web or the Scalefusion Apps.

“Documentation” means the technical user documentation provided with the Services.

“Feedback” means comments, questions, suggestions or other feedback relating to

any ProMobi product or service.

“ProMobi App” means any mobile application or desktop client software included in the applicable Service that is made available by ProMobi.

“Laws” means all applicable local, state, federal and international laws, regulations and conventions, including, without limitation, those related to data privacy and data transfer, international communications, and the exportation of technical or personal data.

“People” (in the singular, “Person”) means Customer’s end user customers, potential customers, and other users of and visitors to the Customer Properties.

“Permitted User” means an employee or Contractor of Customer or its Affiliate who is authorized to access the Service.

“Sensitive Personal Information” means any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards (“PCI DSS”); (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (“HIPAA”); or (iii) any other personal data of an EU citizen deemed to be in a “special category” (as identified in EU Data Protection Directive 95/46/EC or any successor directive or regulation).

“Services” means ProMobi’s proprietary software-as-a-service solution(s), including the Dashboard, Scalefusion application programming interfaces (APIs), Scalefusion Code and Scalefusion Add-on Apps, Scalefusion JavaScript APIs, Scalefusion Developer APIs as described in the applicable purchase order form.

“Taxes” means any sales, use, GST, value-added, withholding, or similar taxes or levies, whether domestic or foreign, other than taxes based on the income of ProMobi.

“Third-Party Platform” means any software, software-as-a-service, data sources or other products or services not provided by ProMobi that are integrated with Services as described in the Documentation.

2. ProMobi Services

2.1. Services Overview: ProMobi’s Services are a suite of mobility software-as-a-service solutions offered through a single platform. The Services are designed to enable Customer to manage their corporate owned devices and to provide a Dashboard for accessing and managing Customer Data regarding those devices. Customer may import and export Customer Data between the Services and certain Third-Party Platforms through supported integrations. The Services also include ProMobi Apps or Code deployed on Customer Properties (i.e devices) to enable management functionality.

2.2. Provision of Services: Each Service is provided on a subscription basis for a set term designated on the purchase order form (each, a “Subscription Plan”). ProMobi may also offer Professional Services (as defined in Section 11) related to certain Services. Customer will purchase and ProMobi will provide the specific Services and related Professional Services (if any) as specified in the applicable purchase order form.

2.3. Access to Services: Customer may access and use the Services solely for its own benefit and in accordance with the terms and conditions of this Agreement, the Documentation and any scope of use restrictions designated in the applicable purchase order form (including without limitation the number of devices managed). Use of and access to the Services is permitted only by Permitted Users. If Customer is given API keys or passwords to access the Services on ProMobi's systems, Customer will require that all Permitted Users keep API keys, user ID and password information strictly confidential and not share such information with any unauthorized person. User IDs are granted to individual, named persons and may not be shared. If Customer is accessing the Services using credentials provided by a third party (e.g., Google), then Customer will comply with all applicable terms and conditions of such third party regarding provisioning and use of such credentials. Customer will be responsible for any and all actions taken using Customer's accounts and passwords. If any Permitted User who has access to a user ID is no longer an employee (or Contractor, as set forth below) of Customer, then Customer will immediately delete such user ID and otherwise terminate such Permitted User's access to the Service. The right to use the Services includes the right to deploy ProMobi Apps and Code on Customer Properties in order to enable device management, monitoring and similar functionality and to collect Customer Data for use with the Services as further described below.

2.4. ProMobi Apps: To the extent ProMobi provides ProMobi Apps for use with the Services, subject to all of the terms and conditions of this Agreement, ProMobi grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to use the object code form of the ProMobi Apps internally, but only in connection with Customer's use of the Service and otherwise in accordance with the Documentation and this Agreement.

2.5. Deployment of ProMobi Apps: Subject to all of the terms and conditions of this Agreement, ProMobi grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to deploy the ProMobi Apps in the form provided by ProMobi on Customer Properties solely to support Customer's use of the Service and otherwise in accordance with the Documentation and this Agreement. Customer must install ProMobi Apps on the Customer Properties in order to enable features of the Services. Customer will deploy all ProMobi Apps in strict accordance with the Documentation and other instructions provided by ProMobi. Customer acknowledges that any changes made to the Customer Properties after initial deployment of ProMobi Code may cause the Services to cease working or function improperly and that ProMobi will have no responsibility for the impact of any such Customer changes.

2.6. Contractors and Affiliates: Customer may permit its Contractors and its Affiliates' employees and Contractors to serve as Permitted Users, provided Customer remains responsible for compliance by such individuals with all of the terms and conditions of this Agreement, and any use of the Services by such individuals is for the sole benefit of Customer.

2.7. General Restrictions: Customer will not (and will not permit any third party to): (a) rent, lease, provide access to or sublicense the Services to a third party; (b) use the Services to provide, or incorporate the Services into, any product or service provided to a third party; © reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to the Services, except to the extent expressly permitted by applicable law (and then only upon advance notice to ProMobi); (d) copy or modify the Services or any Documentation, or create any

derivative work from any of the foregoing; (e) remove or obscure any proprietary or other notices contained in the Services (including without limitation (i) the “Powered by Scalefusion” designation that may appear as part of the deployment of the Services on Customer Properties and (ii) notices on any reports or data printed from the Services); or (f) publicly disseminate information regarding the performance of the Services.

2.8. Scalefusion APIs: If ProMobi makes access to any APIs available as part of the Services, then ProMobi reserves the right to place limits on access to such APIs (e.g., limits on numbers of calls or requests). Further, ProMobi may monitor Customer’s usage of such APIs and limit the number of calls or requests Customer may make if ProMobi believes that Customer’s usage is in breach of this Agreement or may negatively affect the Services (or otherwise impose liability on ProMobi).

2.9. Trial Subscriptions: If Customer receives free access or a trial or evaluation subscription to the Service (a “Trial Subscription”), then Customer may use the Services in accordance with the terms and conditions of this Agreement for a period of fourteen (14) days or such other period granted by ProMobi (the “Trial Period”). Trial Subscriptions are permitted solely for Customer’s use to determine whether to purchase a paid subscription to the Services. Trial Subscriptions may not include all functionality and features accessible as part of a paid Subscription Term. If Customer does not enter into a paid Subscription Term, this Agreement and Customer’s right to access and use the Services will terminate at the end of the Trial Period. ProMobi has the right to terminate a Trial Subscription at any time for any reason.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ProMobi WILL HAVE NO WARRANTY, INDEMNITY, SUPPORT, OR OTHER OBLIGATIONS WITH RESPECT TO TRIAL SUBSCRIPTIONS.

3. Customer Data

3.1. Rights in Customer Data: As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data as provided to ProMobi. Subject to the terms of this Agreement, Customer hereby grants to ProMobi a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data solely to the extent necessary to provide the Services to Customer.

3.2. Storage of Customer Data: ProMobi does not provide any long term archiving service. ProMobi agrees only that it will not intentionally delete any Customer Data from any Service prior to termination of Customer’s applicable Subscription Term. ProMobi expressly disclaims all other obligations with respect to storage.

3.3. Customer Obligations

a) *In General* Customer is solely responsible for the accuracy, content and legality of all Customer Data. Customer represents and warrants to ProMobi that Customer has all necessary rights, consents and permissions to collect, share and use all Customer Data as contemplated in this Agreement (including granting ProMobi the rights in Section 3.1 (Rights in Customer Data)) and that no Customer Data will violate or infringe (i) any third party intellectual property, publicity, privacy or other rights, (ii) any Laws, or (iii) any terms of service, privacy policies or other agreements governing the Customer Properties or Customer’s accounts with any Third-Party Platforms. Customer further represents and warrants that all Customer Data complies with the

AUP. Customer will be fully responsible for any Customer Data submitted to the Services by any Person as if it was submitted by Customer.

b) *No Sensitive Personal Information.* Customer specifically agrees not to use the Services to collect, store, process or transmit any Sensitive Personal Information. Customer acknowledges that ProMobi is not a Business Associate or subcontractor (as those terms are defined in HIPAA) or a payment card processor and that the Services are neither HIPAA nor PCI DSS compliant. ProMobi will have no liability under this Agreement for Sensitive Personal Information, notwithstanding anything to the contrary herein.

c) *Compliance with Laws.* Customer agrees to comply with all applicable Laws in its use of the Services. Without limiting the generality of the foregoing, Customer will not engage in any unsolicited advertising, marketing, or other activities using the Services, including without limitation any activities that violate the Telephone Consumer Protection Act of 1991, CAN-SPAM Act of 2003 or any other anti-spam laws and regulations.

3.4. Indemnification by Customer: Customer will indemnify, defend and hold harmless ProMobi from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with any claim arising from or relating to any Customer Data or breach or alleged breach by Customer of Section 3.3 (Customer Obligations). This indemnification obligation is subject to Customer receiving (i) prompt written notice of such claim (but in any event notice in sufficient time for Customer to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense, or settlement of such claim; and (iii) all necessary cooperation of ProMobi at Customer's expense. Notwithstanding the foregoing sentence, (a) ProMobi may participate in the defense of any claim by counsel of its own choosing, at its cost and expense and (b) Customer will not settle any claim without ProMobi's prior written consent, unless the settlement fully and unconditionally releases ProMobi and does not require ProMobi to pay any amount, take any action, or admit any liability.

3.5. Aggregated Anonymous Data: Notwithstanding anything to the contrary herein, Customer agrees that ProMobi may obtain and aggregate technical and other data about Customer's use of the Services that is non-personally identifiable with respect to Customer ("Aggregated Anonymous Data"), and ProMobi may use the Aggregated Anonymous Data to analyze, improve, support and operate the Services and otherwise for any business purpose during and after the term of this Agreement, including without limitation to generate industry benchmark or best practice guidance, recommendations or similar reports for distribution to and consumption by Customer and other ProMobi customers. For clarity, this Section 3.5 does not give ProMobi the right to identify Customer as the source of any Aggregated Anonymous Data.

4. Security

ProMobi agrees to use commercially reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of any Service or Customer Data. However, ProMobi will have no responsibility for errors in transmission, unauthorized third-party access or other causes beyond ProMobi's control. Visit ProMobi's [security practices](#) here.

5. Third-Party Platform Integrations

The Services may support integrations with certain Third-Party Platforms. In order for the Services to communicate with such Third-Party Platforms, Customer may be required to input credentials in order for the Services to access and receive relevant information from such Third-Party Platforms. By enabling use of the Services with any Third-Party Platform, Customer authorizes ProMobi to access Customer's accounts with such Third-Party Platform for the purposes described in this Agreement. Customer is solely responsible for complying with any relevant terms and conditions of the Third-Party Platforms and maintaining appropriate accounts in good standing with the providers of the Third-Party Platforms. Customer acknowledges and agrees that ProMobi has no responsibility or liability for any Third-Party Platform or any Customer Data exported to a Third-Party Platform. ProMobi does not guarantee that the Services will maintain integrations with any Third-Party Platform and ProMobi may disable integrations of the Services with any Third-Party Platform at any time with or without notice to Customer. For clarity, this Agreement governs Customer's use of and access to the Services, even if accessed through an integration with a Third-Party Platform.

6. Ownership

6.1. **Scalefusion Technology_**: This is a subscription agreement for access to and use of the Services. Customer acknowledges that it is obtaining only a limited right to the Services and that irrespective of any use of the words "purchase", "sale" or like terms in this Agreement no ownership rights are being conveyed to Customer under this Agreement. Customer agrees that ProMobi or its suppliers retain all right, title and interest (including all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the Services and all Documentation, professional services deliverables and any and all related and underlying technology and documentation and any derivative works, modifications or improvements of any of the foregoing, including as may incorporate Feedback (collectively, "**Scalefusion Technology**"). Except as expressly set forth in this Agreement, no rights in any **Scalefusion Technology** are granted to Customer. Further, Customer acknowledges that the Services are offered as an on-line, hosted solution, and that Customer has no right to obtain a copy of any of the Services, except for ProMobi Code and the ProMobi Apps in the format provided by ProMobi.

6.2. **Feedback**. Customer, from time to time, may submit Feedback to ProMobi. ProMobi may freely use or exploit Feedback in connection with any of its products or services.

7. Subscription Term, Fees & Payment

7.1. **Subscription Term and Renewals**: Unless otherwise specified on the applicable purchase order, each Subscription Term will have to be renewed explicitly, you will receive an email notification about the expiry of your Subscription Term at least thirty (30) days prior to expiration of the then-current Subscription Term.

7.2. **Fees and Payment**: All fees are as set forth in the applicable purchase order and will be paid by Customer within thirty (30) days of invoice, unless (a) Customer is paying via Credit Card (as defined below) or (b) otherwise specified in the applicable purchase order. Except as expressly set forth in Section 9 (Limited Warranty) and Section 14 (Indemnification), all fees are non-refundable. The rates in the purchase

order and/or invoices are valid for the initial twelve (12) month period of each Subscription Term and thereafter may be subject to an automatic adjustment increase of up to ten percent (10%) per year. Customer is responsible for paying all Taxes, and all Taxes are excluded from any fees set forth in the applicable purchase order. If Customer is required by Law to withhold any Taxes from Customer's payment, the fees payable by Customer will be increased as necessary so that after making any required withholdings, ProMobi receives and retains (free from any liability for payment of Taxes) an amount equal to the amount it would have received had no such withholdings been made. Any late payments will be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less.

7.3. Payment Via Credit Card: If you are purchasing the Services via credit card, debit card or other payment card ("Credit Card"), the following terms apply:

- **Foreign Transaction Fees.** Customer acknowledges that for certain Credit Cards, the issuer of Customer's Credit Card may charge a foreign transaction fee or other charges.
- **Invalid Payment:** If a payment is not successfully settled due to expiration of a Credit Card, insufficient funds, or otherwise, Customer remains responsible for any amounts not remitted to ProMobi and ProMobi may, in its sole discretion, either (i) invoice Customer directly for the deficient amount, or (ii) terminate the Subscription Term as well as this Agreement.
- **Payment of Outstanding Fees.** Upon any termination or expiration of the Subscription Term, ProMobi will invoice Customer directly for any outstanding fees for Customer's use of the Services during the Subscription Term, after which ProMobi will not charge for any additional fees, once the outstanding amount is paid in full.

7.4. Suspension of Service. If Customer's account is thirty (30) days or more overdue, in addition to any of its other rights or remedies (including but not limited to any termination rights set forth herein), ProMobi reserves the right to suspend Customer's access to the applicable Service (and any related services) without liability to Customer until such amounts are paid in full. ProMobi also reserves the right to suspend Customer's access to the Services without liability to Customer if Customer's use of the Services is in violation of the AUP.

7.5. Subscription Downgrade. Customer cannot downgrade their plan in the middle of an existing active subscription. However, customers can downgrade their plan at the renewal of their existing subscription. The newly chosen plan will be effective only after the renewal. Customers can choose to downgrade to the then-available subscription plan while renewal.

7.6. Subscription Plan. ProMobi reserves the right to change its offering of subscription plans, including by limiting or ceasing to offer any subscription plans, including any associated features as well, upon sending a written notice to Customer, which may be by email. Subscription plans may not be available to all customers and regions.

8. Term and Termination

8.1. Term. This Agreement is effective as of the Effective Date and expires on the date of expiration or termination of all Subscription Terms.

8.2. Termination for Cause. Either party may terminate this Agreement (including all related purchase orders) if the other party (a) fails to cure any material breach of this Agreement (including a failure to pay fees) within thirty (30) days after written notice; (b) ceases operation without a successor; or (c) seeks protection under any bankruptcy, receivership, trust deed, creditors' arrangement, composition, or comparable proceeding, or if any such proceeding is instituted against that party (and not dismissed within sixty (60) days thereafter).

8.3. Effect of Termination. Upon any expiration or termination of this Agreement, Customer will immediately cease any and all use of and access to all Services (including any and all related Scalefusion Technology) and delete (or, at ProMobi's request, return) any and all copies of the Documentation, any Scalefusion passwords or access codes and any other ProMobi Confidential Information in its possession. Provided this Agreement was not terminated for Customer's breach, Customer may retain and use internally copies of all reports exported from any Service prior to termination. Customer acknowledges that following termination it will have no further access to any Customer Data input into any Service, and that ProMobi may delete any such data as may have been stored by ProMobi at any time. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law or otherwise.

8.4. Survival. The following Sections will survive any expiration or termination of this Agreement: 2.7 (General Restrictions), 2.9 (Trial Subscriptions), 3.2 (Storage of Customer Data), 3.4 (Indemnification by Customer), 3.5 (Aggregated Anonymous Data), 6 (Ownership), 7.2 (Fees and Payment), 7.3 (Payment Via Credit Card), 8 (Term and Termination), 9.2 (Warranty Disclaimer), 12 (Limitation of Remedies and Damages), 13 (Indemnification), 14 (Confidential Information) and 16 (General Terms).

9. Limited Warranty

9.1. Limited Warranty: ProMobi warrants, for Customer's benefit only, that each Service will operate in substantial conformity with the applicable Documentation. ProMobi's sole liability (and Customer's sole and exclusive remedy) for any breach of this warranty will be, at no charge to Customer, for ProMobi to use commercially reasonable efforts to correct the reported non-conformity, or if ProMobi determines such remedy to be impracticable, either party may terminate the applicable Subscription Term and Customer will receive as its sole remedy a refund of any fees Customer has pre-paid for use of such Service for the terminated portion of the applicable Subscription Term. The limited warranty set forth in this Section 9.1 will not apply: (i) unless Customer makes a claim within thirty (30) days of the date on which Customer first noticed the non-conformity, (ii) if the error was caused by misuse, unauthorized modifications or third-party hardware, software or services, or (iii) to use provided on a no-charge, trial or evaluation basis.

9.2. Warranty Disclaimer: EXCEPT FOR THE LIMITED WARRANTY IN SECTION 9.1, ALL Services and PROFESSIONAL SERVICES ARE PROVIDED "AS IS". NEITHER PROMOBI NOR ITS SUPPLIERS MAKES ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. ProMobi does not warrant that Customer's use of THE Services will be uninterrupted or error-free, nor does ProMobi

warrant that it will review the Customer Data for accuracy or that it will preserve or maintain the Customer Data without loss OR CORRUPTION. PROMOBI SHALL NOT BE LIABLE FOR THE RESULTS OF ANY COMMUNICATIONS SENT OR ANY COMMUNICATIONS THAT WERE FAILED TO BE SENT USING THE SERVICES. ProMobi SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES OR OTHER PROBLEMS INHERENT IN USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS, THIRD-PARTY PLATFORMS OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF ProMobi. CUSTOMER MAY HAVE OTHER STATUTORY RIGHTS, BUT THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE SHORTEST PERIOD PERMITTED BY LAW.

10. Support

During the Subscription Term of each Service, ProMobi will provide end user support in accordance with ProMobi's [Support Policy](#) ("Support Policy").

11. Professional Services

ProMobi may provide the professional consulting services ("Professional Services") purchased in the applicable purchase order. The scope of Professional Services will be as set forth in a Statement of Work ("SOW") referencing this Agreement and executed by both parties describing the work to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information ("SOW"). Unless Professional Services are provided on a fixed-fee basis, Customer will pay ProMobi at the per-hour rates set forth in the Purchase Order Form (or, if not specified, at ProMobi's then-standard rates) for any excess services. Customer will reimburse ProMobi for reasonable travel and lodging expenses as incurred. Customer may use anything delivered as part of the Professional Services in support of authorized use of the Services and subject to the terms regarding Customer's rights to use the Service set forth in Section 2 (ProMobi Services) and the applicable SOW, but ProMobi will retain all right, title and interest in and to any such work product, code or deliverables and any derivative, enhancement or modification thereof created by ProMobi (or its agents).

12. Limitation of Remedies and Damages

12.1. Consequential Damages Waiver. EXCEPT FOR EXCLUDED CLAIMS (DEFINED BELOW), NEITHER PARTY (NOR ITS SUPPLIERS) SHALL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOSS OF USE, LOST DATA, LOST PROFITS, FAILURE OF SECURITY MECHANISMS, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12.2. Liability Cap. PROMOBI'S AND ITS SUPPLIERS' ENTIRE LIABILITY TO CUSTOMER ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY CUSTOMER TO PROMOBI DURING THE PRIOR TWELVE (12) MONTHS UNDER THIS AGREEMENT.

12.3. Excluded Claims. "Excluded Claims" means any claim arising (a) from Customer's breach of Section 2.7 (General Restrictions); (b) under Section 3.3 (Customer Obligations) or 3.4 (Indemnification by Customer); or © from a party's

breach of its obligations in Section 15 (Confidential Information) (but excluding claims arising from operation or non-operation of any Service).

12.4. Nature of Claims and Failure of Essential Purpose. The parties agree that the waivers and limitations specified in this Section 13 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy specified in this Agreement is found to have failed of its essential purpose.

13. Indemnification

ProMobi will defend Customer from and against any claim by a third party alleging that a Service when used as authorized under this Agreement infringes a U.S. patent, U.S. copyright, or U.S. trademark and will indemnify and hold harmless Customer from and against any damages and costs finally awarded against Customer or agreed in settlement by ProMobi (including reasonable attorneys' fees) resulting from such claim, provided that ProMobi will have received from Customer: (i) prompt written notice of such claim (but in any event notice in sufficient time for ProMobi to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense and settlement (if applicable) of such claim; and (iii) all reasonable necessary cooperation of Customer. If Customer's use of a Service is (or in ProMobi's opinion is likely to be) enjoined, if required by settlement or if ProMobi determines such actions are reasonably necessary to avoid material liability, ProMobi may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for Customer the right to continue using such Service; or if (a) and (b) are not commercially reasonable, © terminate this Agreement and refund to Customer the fees paid by Customer for the portion of the Subscription Term that was paid by Customer but not rendered by ProMobi. The foregoing indemnification obligation of ProMobi will not apply: (1) if such Service is modified by any party other than ProMobi, but solely to the extent the alleged infringement is caused by such modification; (2) if such Service is combined with products or processes not provided by ProMobi, but solely to the extent the alleged infringement is caused by such combination; (3) to any unauthorized use of such Service; (4) to any action arising as a result of Customer Data or any third-party deliverables or components contained within such Service; (5) to the extent the alleged infringement is not caused by the particular technology or implementation of the Service but instead by features common to any similar product or service; or (6) if Customer settles or makes any admissions with respect to a claim without ProMobi's prior written consent. THIS SECTION 13 SETS FORTH ProMobi's AND ITS SUPPLIERS' SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

14. Confidential Information

Each party (as "**Receiving Party**") agrees that all code, inventions, know-how, business, technical and financial information it obtains from the disclosing party ("**Disclosing Party**") constitute the confidential property of the Disclosing Party ("**Confidential Information**"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be confidential or proprietary due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any Scalefusion Technology, performance information relating to any Service, and the terms and conditions of this Agreement will be deemed Confidential Information of ProMobi without any marking or further

designation. Except as expressly authorized herein, the Receiving Party will (1) hold in confidence and not disclose any Confidential Information to third parties and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement. The Receiving Party may disclose Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know (including, for ProMobi, the subcontractors referenced in Section 17.8 (Subcontractors)), provided that such representatives are bound to confidentiality obligations no less protective of the Disclosing Party than this Section 14 and that the Receiving Party remains responsible for compliance by any such representative with the terms of this Section 14. The Receiving Party's confidentiality obligations will not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information. The Receiving Party may make disclosures to the extent required by law or court order, provided the Receiving Party notifies the Disclosing Party in advance and cooperates in any effort to obtain confidential treatment. The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

15. Co-Marketing

At the request of ProMobi, Customer may agree to participate in other reasonable marketing activities that promote the benefits of the Services to other potential customers and to use of Customer's name and logo on ProMobi's web site and in ProMobi promotional materials. Customer agrees that ProMobi may disclose Customer as a customer of ProMobi.

16. General Terms

16.1. Assignment: This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in connection with a merger, reorganization, acquisition or other transfer of all or substantially all of such party's assets or voting securities. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section 16.1 will be null and void.

16.2. Severability: If any provision of this Agreement will be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect.

16.3. Entire Agreement: This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement. Customer acknowledges that the Services are on-line, subscription-based products, and that in order to provide improved customer experience ProMobi

may make changes to the Services, and ProMobi will update the applicable Documentation accordingly. The support terms described in the Support Policy may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices (but the modifications will not materially decrease ProMobi's obligations as compared to those reflected in such terms as of the Effective Date).

16.4. Force Majeure: Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events that occur after the signing of this Agreement and that are beyond the reasonable control of such party, such as a strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or telecommunications or data networks or services, or refusal of a license by a government agency.

16.5. Subcontractors: ProMobi may use the services of subcontractors and permit them to exercise the rights granted to ProMobi in order to provide the Services under this Agreement, provided that ProMobi remains responsible for (i) compliance of any such subcontractor with the terms of this Agreement and (ii) for the overall performance of the Services as required under this Agreement.

16.6. Subpoenas: Nothing in this Agreement prevents ProMobi from disclosing Customer Data to the extent required by law, subpoenas, or court orders, but ProMobi will use commercially reasonable efforts to notify Customer where permitted to do so.

16.7 Changes to this Agreement. We may update or modify this Agreement from time to time, including any referenced policies and other documents. If a revision meaningfully reduces your rights, we will use reasonable efforts to notify you (by, for example, sending an email to the billing or technical contact you designate in the applicable purchase Order, posting on our blog, through your ProMobi account, or in the Product itself). If we modify the Agreement during your License Term or Subscription Term, the modified version will be effective upon your next renewal of a License Term, Support and Maintenance term, or Subscription Term, as applicable. In this case, if you object to the updated Agreement, as your exclusive remedy, you may choose not to renew, including cancelling any terms set to auto-renew. With respect to No-Charge Products, accepting the updated Agreement is required for you to continue using the No-Charge Products. You may be required to click through the updated Agreement to show your acceptance. If you do not agree to the updated Agreement after it becomes effective, you will no longer have a right to use No-Charge Products. For the avoidance of doubt, any purchase Order is subject to the version of the Agreement in effect at the time of the Order.

16.8. Counterparts: This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

ACCELERATING BUSINESS WITH SPOORS – EFFORT FIELD SERVICE MANAGEMENT IN THE CLOUD

If your business need advance functionalities for managing Service orders, Dispatching technicians, Work planning, Route optimization Effort is the product. Built for the cloud, Effort Field Service Management has enabled staff to work on the go, helping the highest performing service organizations tackle a new generation of field service challenges.

Cloud solutions to field service management means there's no infrastructure to manage, making it easy to provision new operations, upscale or add more functionalities as soon as you need it.

Cloud-based solutions are very attractive for field service because they may be more flexible, readily extensible and more accessible being cost effective.



High on Configurability

The advantages of using effort is the enhanced operational flexibility and agility it gives your business. Our cloud services support options for configuration, customization & integrations and it provides the choice of when to deploy updates, except for mandatory essential patches.

Unique Value proposition

1. Dynamic Mobile **Form engine**
2. **Offline Mobile App** for IOS & Android Devices
3. Flexibility to Capture Images, Videos, Audio
4. **Geotagging** of Activities



GENERAL TERMS AND CONDITION

- Signup/registration on the Website/App is available only to the person who can form legally binding contracts under Indian Contract Act, 1872. Persons who are "incompetent to contract" within the meaning of the Indian Contract Act, 1872 including minors, un-discharged insolvents etc. are not eligible to register on the Website/App. As a minor if User wish to use the Website/App, shall be registered by legal guardian or parents on the Website/App. If it comes to the knowledge of Spoors Private Limited that the User registered on the Website/App via providing the personal information is under the age of 18 years, shall be removed from the Website/App by Spoors Private Limited. Spoors Private Limited reserves the right to terminate the membership and / or refuse to provide the User with access to the Website/App if it is brought to Spoors Private Limited notice or if it is discovered that the signup/registration over the Website/App is done by a User, under the age of 18 years.
- Signup/registration of the User on the Website/App is necessary to access the Website/App and use the services. User shall be required to signup/register for an account on the Website/App by providing email address, name, password and user name. User shall provide accurate, complete and updated information in order to signup/register on the Website/App to use the services.
- User represent, warrant, and agree that User shall not use the services in a manner that:
 1. Infringes or violates the intellectual property rights or any other rights of anyone else.
 2. Violates any law or regulation;
 3. Is harmful, fraudulent, deceptive, threatening, harassing, defamatory, obscene, or otherwise objectionable;

4. Attempts, in any manner, to obtain the password, account, or other security information from any other User;
 5. Violates the security of any computer network, or cracks any passwords, or security encryption codes;
- User accepts the Website/App Terms and condition, Privacy Policy by using the “OTP” to signup/register when registering and logging into the Website/App to use the services.
 - Spoors Private Limited might change the methodology or functionality of the Website/App at any point of time and intimation to that extent shall be mentioned in the Website/App under Terms and Conditions.
 - Spoors Private Limited shall always try to improve the services provided by the Website/App which shall include suspension or discontinuation of any part of the services. Spoors Private Limited shall introduce features or impose limit on certain features or restrict access to parts or all of the services provided through the Website/App. A notification of any such action shall be sent to the User in advance.
 - Spoors Private Limited reserves the right to remove any content provided on the Website/App at any time without any reason or any notice of any such action by Spoors Private Limited on the Website/App. Subject to the terms and conditions set forth in this Agreement. Spoors Private Limited grants User a non-exclusive, non-transferable, limited right to access and use this Website/App and the information thereon. User agrees not to interrupt or attempt to interrupt the services of the Website/App in any way.
 - The information provided on the Website/App are in relation to providing services such as text, graphics, article, photos, images are protected by the Copyright and other Intellectual Property Laws. User promises to abide by all Copyright notices, Trademark rules and the User won't use, copy, reproduce, modify, translate, publish, broadcast, transmit, distribute, perform, upload, display, license, sell or otherwise exploit for any purpose any Content not owned by the User without the prior written consent of Spoors Private Limited. User won't modify, publish, transmit, participate in the transfer or sale

of, reproduce, create derivative works based on, or otherwise exploit any of the Services.

- The information on this Website/App has been included in good faith and is for general purposes only. It should not be relied upon for any specific purpose and no representation or warranty is given as regards its accuracy or completeness.
- No reproduction of any part of the Website/App may be sold or distributed for commercial gain, nor shall it be modified or incorporated in any other work, publication or site, whether in hard copy or electronic format, including postings to any other site. Spoors Private Limited reserves all other rights.
- Neither Spoors Sons and Spoors affiliates, nor their affiliates' officers, employees or agents shall be liable for any loss, damage or expense arising out of any access to or use of this Website/App including without limitation, any loss of profit, indirect, incidental or consequential loss.
- In relation to any circumstances that arise due to the Use of the Website/App shall be communicated to the customer care of the Website/App. User understands that there may be instances of difficulty in accessing or receiving email communication. We are not responsible if any email notice gets caught by User's SPAM folder, or if User do not see the email, or if User has given us an incorrect email id or if for any other reason You do not receive the email notice. Therefore, we encourage User to frequently open the Application to monitor any changes. User continued use of or access to the Services following the posting of any changes to this Agreement constitutes acceptance of those changes.
- Any failure of functioning of the Website/App shall be intimated by the User to Spoors Private Limited and Spoors Private Limited shall duly try to resolve the issue. Spoors Private Limited shall not be liable for any kind of damages or losses faced by the User due to functionality of the Website/App.

- Payment of such services shall be in accordance to the charges available on the app store during purchase of such services, or as informed by Spoors Private Limited to the User based on the services availed.
- Spoors Private Limited will protect the data to the extent required by applicable law, and subject to applicable law, Spoors Private Limited will take every security measure for protection of the data provided. Spoors Private Limited will not disclose any information to any third-party and will not engage directly with another processor to provide the Services to the User. Spoors Private Limited will keep records of its processing activities with respect to any data and cooperate with authorized person in respect of any complaint or investigation relating to such data. Website/App will notify the User in respect of any suspected or actual breach of data security or other unauthorized access or processing of any such data .
- User agrees to indemnify and hold Spoors Private Limited, its affiliates, officers, agents, employees, and partners harmless for and against any and all claims, liabilities, damages (actual and consequential), losses and expenses (including attorneys' fees) arising from or in any way related to any third party claims relating to (a) User's use of the Services (including any actions taken by a third party using User account), and (b) User's violation of these Terms. In the event of such a claim, suit, or action, Spoors Private Limited shall provide notice of the claim to the contact information provided by the User during signup/registration on the Website/App. Failure to deliver such notice shall not eliminate or reduce User's indemnification obligations hereunder.
- Spoors Private Limited shall own all rights, title, and interest in the feedback provided by the User and Spoors Private Limited shall be entitled to use the feedback without restriction, even if the User has indicated such feedback as confidential or restricted for improvement of Website/App services. Website/App shall not be under any obligation of confidentiality, express or implied, with respect to the feedback. Spoors Private Limited shall be entitled to use or disclose any such feedback for any purpose, in any

way required and Spoors Private Limited will not be liable for any compensation for any such disclosure under any circumstances.

- Spoors Private Limited will suspend the Users right to use the services immediately upon notice of any security risk due to the Users use of the services which may impact the App or other systems or if it comes to the knowledge of any fraudulent use of Website/App.
- This Agreement is the complete and exclusive statement of the agreements between User and Spoors Private Limited with respect to the subject matter hereof and supersedes all other communications or representations or agreements (whether oral, written or otherwise) relating thereto.
- The failure of either party at any time to require performance of any provision of this Agreement in no manner shall affect such party's right at a later time to enforce the same. No waiver by either party of any breach of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be, or construed as, a further or continuing waiver of any other such breach, or a waiver of any other breach of this Agreement.
- If any provision of this Agreement shall to any extent be held invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions of this Agreement shall in no way be affected or impaired thereby and each such provision of this Agreement shall be valid and enforceable to the fullest extent permitted by law. In such case, this Agreement shall be reformed to the minimum extent necessary to correct any invalidity, illegality or unenforceability, while preserving to the maximum extent the rights and commercial expectations of the parties hereto, as expressed herein.
- These Terms are governed by and will be construed under the laws of India, without regard to the conflicts of laws provisions thereof, unless prohibited by law. Any dispute arising from or relating to the subject matter of these Terms shall be finally settled in

Hyderabad, India. THIS CLAUSE SHALL SURVIVE THE TERMINATION OR EXPIRY OF THIS AGREEMENT.

- **I AGREE TO THE ABOVE TERMS AND CONDITIONS**

Attachment:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory D: Workforce Management

Subcategory E: Field Service Management

Client Company name:	Mama Bear in Home Care
Client name of contact:	Valerie Johnson
Client contact title:	Owner & CEO
Client is a daily user, occasional user, etc.:	Daily User

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to James Rose no later than Friday, November 6th.

Thank you for your assistance in this process.

- 1. For what services do you use USCC's product, and how long have you been USCC's customer?**
doForms
- 2. Would you recommend USCC to other customers? Why?**
Yes, they worked with me to get everything done exactly the way I needed it, very happy with everyone I've dealt with.
- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services?**

How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

Did everything to make DoForms to run smoothly and when we had issues US Cellular put us with someone else who was able to help better, without making the us feel bad.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

Way exceed expectations, dealt with me even when I'm cranky. Held my hand even when she's confused with technical issues.
- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

DoForms wasn't as easy to use as originally shown, but they worked with me until it was right. My employees and I use them every day now.
- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

N/A Absolutely love USCC
- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

I Think US Cellular people are awesome and patient.
- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

80 tablets and currently implementing Mass 360. I also like that I have one bill for everything through US Cellular.

Appendix J

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory F: Mobile Data Collection / Mobile Forms

doForms



NASPO

ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
doForms – doForms Mobile Data Collection Solution with Mobile Forms, Dispatch and Tracking
- b. General Application Area
Subcategory F: Mobile Data Collection/Mobile Forms
- c. General capabilities provided
doForms is a highly flexible and scalable mobile data collection solution that provides customers with the ability to quickly build, deploy and collect customized mobile forms. Forms can be as simple or complex as required with a very user intuitive interface. Form capabilities include but not limited to lookup tables, if then else logic, GPS stamps/tracking, email workflow, form forwarding, media capture (audio, images, signatures, sketches, and video), support for offline (store & forward) scenarios, and much more. doForms is easily installed on supported Apple iOS or Google Android mobile devices in minutes with additional support for web-based forms. Mobile forms are auto responsive to any device screen size out of the box with optional customization of scrolling or panning of forms.
- d. Expected impact on cost/performance/functionality, etc.
doForms is licensed per mobile or web user with unlimited forms, projects and data collection. Depending upon the size, complexity and information collected, impact to standard data plans is minimal. Customers requiring high volumes of hi-resolution photographs or video capture may consider a higher data plan.
- e. Subcontractors/partners involved in delivering service
doForms provides all sales, support and training unless third-party contractors are required by the customer.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, see the following:
 - EULA - <https://www.doforms.com/eula/>
 - Privacy Policy - <https://www.doforms.com/privacy-policy/>
 - Terms of Use - <https://www.doforms.com/terms-of-use/>

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
At a high level, the doForms mobile data collection solution consists of three components:
 - doForms Web Portal (dashboard) – Administration of the doForms licensed users, forms, projects, reporting, security, branding, etc...
 - doForms Mobile Application – Supports Apple iOS and Google Android mobile devices with additional flexibility for data collection using web browser forms.

- Optional Integration – doForms web services (programmatic) or integration products (automated) are available for customers that need to export doForms collected data to back office systems including but not limited to QuickBooks, SharePoint, Salesforce.com, SQL Server, Oracle, etc...
- b. Applicability to government needs
- doForms implements security with encryption of all data communication over SSL or TLS1.2 at a minimum of AES 256. Data at rest in the doForms cloud is FIPS certified to be encrypted at rest. Customers can enable advanced security measures such as complex password, email multi-factor authentication, user lock-out, etc. The doForms solution is hosted and powered by the Google Cloud Platform which includes the Google App Engine (GAE), Google datastore and other Google services. The Google Cloud Platform compliances includes SOC1 (SSAE-16/ISAE-3402), SOC2, SOC3, ISO27001, ISO27017, ISO27018, HIPAA, FISMA, PCI-DSS, C-STAR, etc.
- <https://cloud.google.com/security/compliance/soc-1/>
 - <https://cloud.google.com/security/compliance/soc-2/>
 - <https://cloud.google.com/security/compliance/soc-3/>
 - <https://cloud.google.com/security/compliance/iso-27001/>
 - <https://cloud.google.com/security/compliance/iso-27017/>
 - <https://cloud.google.com/security/compliance/iso-27018/>
 - <https://cloud.google.com/security/compliance/pci-dss/>
 - <https://cloud.google.com/security/compliance/csa-star>
- No doForms employee, partner, reseller, contractor or subcontractor has access to any Google data center. No platform infrastructure is located or hosted at any doForms office. As such, no customer data is located or stored at any doForms office.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
- doForms is a single mobile data collection solution that customers can customize to meet their needs. This includes fulling customizable and scalable mobile forms, extensive branding of the doForms web portal/mobile forms/mobile applications, easy configuration of licensed user access, etc.
- d. Overall interoperability of turnkey system for government use
- The doForms web portal and web forms support the four major web browsers (Chrome, Firefox, Internet Explorer and Safari) and required an internet connection. The doForms mobile application supports Apple iOS and Google Android mobile devices and requires an internet connection to authorize, download and submit forms with the support of offline (store & forward) scenarios.
- e. Accessories available for turnkey offering
- doForms has partnered with and provides mobile application support hardware vendors providing Bluetooth printers and handheld scanners.
- f. Thoroughness of the vetting process used to select partners
- doForms only partners with well-established and long-standing companies such as US Cellular, Brother, Honeywell and Zebra who find mutual benefit with a partnership and/or integration.

- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
doForms third party hardware partners with Brother, Honeywell, and Zebra undergo integration certification which may include marketing materials or campaigns.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
doForms will provide system and mobile application requirements. doForms suggests customer testing and verification on required mobile hardware especially if using ruggedized devices with modified mobile operations systems. These ruggedized devices may have altered or limited functionality of some specific capabilities versus general off the shelf devices.
- b. Project coordination
doForms mobile solution consultants (MSC) provide pre-sales and ongoing coordination and escalation for general support. Integration support will be assigned to doForms support team manager for escalation and resolution.
- c. Installation and Testing process
doForms mobile solution consultants (MSC) will work with US Cellular and the customer during the installation and testing process including the customization or development of mobile forms.
- d. Client Infrastructure and support assessment process
doForms requires include a supported web browser with internet access and mobile devices running either Apple iOS or Google Android with internet access. The customer's mobile forms can be tested on the mobile devices and submitted for review on the doForms web portal. doForms support phone numbers and email addresses will be provided.
- e. End user Acceptance process
doForms mobile solution consultations (MSC) will work with US Cellular and the customer during the end user acceptance process which typically is the acceptance of the mobile forms, data collection testing or optional integration.
- f. Approach to maintenance and support
doForms typically provides one or two major product releases per year with enhancements, updates or fixes provided each quarter. Any fixes with high severity to customers are resolved and deployed as quickly as possible.
- g. Initial and Ongoing Training provided
doForms provides initial training which may include train the trainer. Ongoing or specific topic may be requested or purchased by the hour as needed. Training videos are available to all customers and provided where applicable for new features.

- h. On-going support and enhancement over the life of the agreement
doForms free standard support and free enhancements/upgrades to all customers during the life of the account. Some customers opt to purchase custom development for company specific or unique feature requirements. This may include exclusive or customer specific integrations.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
Outside of the standard doForms mobile solution, optional integration, training and customization are available. Customer without the time or resources may engage doForms to build all of their forms and provide additional customized training.
- b. Experience and qualifications of partners and subcontractors
doForms provides training and support materials for any partner. Subcontractors are typically engaged at the customer's request and are subsequently trained to meet customer requirements. Otherwise, customers may engage and train any subcontractors on the doForms solution presuming they are licensed accordingly.
- c. Description of Additional Integration and Consulting Services provided
doForms integration offers integration with our web services and Sync & Save integration utility. Web services offers customers with IT or development staff the ability to programmatically develop custom integration to meet specific requirements. doForms Sync & Save is a utility application that can run on any Microsoft Windows laptop, desktop or server. Sync & Save can securely communicate with the doForms cloud and the customer's back-office applications or systems. Sync & Save can integration with Microsoft Products (Access, Excel, SQL Server, or SharePoint), Quick Books, Salesforce.com, relational databases (MySQL, Oracle, SQL Server, Sybase ASE, or ODBC), text files (CSV, TXT, XML), etc.

Appendix K

The State of Utah

In conjunction with NASPO ValuePoint

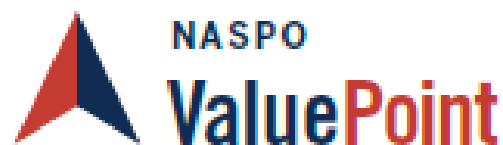
Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Category F: Mobile Data Collection / Mobile Forms

StreamWIDE



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
Team on the Run by StreamWIDE
- b. General Application Area
Subcategory F: Mobile Data Collection/Mobile Forms
- c. General capabilities provided
Team on the Run is a business process communication tool for smartphones, tablets, and PCs. It includes the “My Business”, a flexible process management function with a studio to create custom forms and processes aligned with existing organization workflows. My Business is configurable and scalable deployed on a SaaS model.

Key My Business Features:

- Built in process management Web studio
 - o Define process form layout with user friendly drag and drop capabilities
 - o Manage process and form templates, segment process/form publication to relevant teams or individuals based on business workflow
 - o Define workflow steps and routing to designated supervisors
 - o Create processes and forms out of existing widget toolbox/catalog to collect data in the form of:
 - Address including GPS location captured from device
 - Date and time
 - Phone numbers
 - Currency data
 - General text
 - Check box (Digital checklist)
 - Start and stop time of a task
 - QR code and Barcode decoding
 - NFC data reading (Android devices only)
 - Capture signature
 - Attach pictures, videos
 - Feed data from external systems (additional integration fees may apply)
- Generate reports for data collected from processes and forms
 - o Filter data by template or specific user out of all collected data
 - o Export data to Excel spreadsheet
 - o Generate PDF view
- Process workflow execution traceability
- Process / form data collection
 - o iOS / Android devices
 - o Web desktop interface

Additional communication capabilities that complement My Business:

- Integrated contact list controlled by administrator
- Secured IP messaging integrated with My business processes and forms

- Secured Push-To talk function
 - Secured VOIP calling function
 - Geo-location tracking
- d. Expected impact on cost/performance/functionality, etc.
- Increase productivity by enabling digital collection and flow of business information
 - Reduce operational cost / expenses by implementation of digital forms to collect, transfer and report data in a cohesive process.
 - o Digitalize existing process and forms
 - o Reduce or eliminate paper and duplicated data entry
 - Improve customer satisfaction
 - o Implement digital checklist to reduce errors or quality control
 - o Corrective actions based on increased reporting accuracy
 - Enable an all in one business communication tool
 - o Process management
 - o Secured messaging, text, pictures, videos, audio notes
 - o VOIP calling
 - o Push-To Talk communication
- e. Subcontractors/partners involved in delivering service
UScellular distributes Team on the Run SaaS. Team on the Run is a product developed by StreamWIDE, StreamWIDE team is responsible for implementation (delivery) and support.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes. Please see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
Team on the Run allows organizations to:
- Enhance field and back office teams' productivity
 - Reduce process friction by implementing digital forms
 - Increase quality by using digital checklist
 - Enable business decisions based on more accurate data and reporting
 - Reduce security incidents
 - Provide instant expertise sharing between remote teams
 - Improve P&L
 - Save on communication costs (SMS blast, roaming)
 - Accelerate incidents qualification reporting on the field
 - Have more accurate incidents qualification due to multimedia sharing capabilities

- Achieve faster response and repair time
- Increase organization's customer satisfaction

b. Applicability to government needs

Since data confidentiality and security are a key aspect of the government entities communication process, Team on the Run provides a secure and fully controlled environment to the local, state and federal government staff in the office or in the field; allowing them to communicate via smartphones and tablets.

c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use. Provide references

UScellular provides Team on the Run to 30 active customers with over 400 licenses. StreamWIDE has 150+ organizations utilizing Team on the Run SaaS in US with a total of 10,000+ active end users.

Municipalities

City of Oldbridge Township
Downtown Schenectady
Downtown DC
Tampa Downtown

School districts

Vallejo Unified school district
Washington Unified school district
Richmond Public school VA

d. Overall interoperability of turnkey system for government use

With its key features, 99.999% guaranteed uptime SLA and military-grade secured communication Team on the Run is capable of fulfilling any state, local and federal government secure messaging needs.

The solution is deployed on a SaaS/ cloud model and requires:

- Mobile devices Android / iOS with 3G/4G/5G data plan for mobile users
- Desktop with Chrome/Firefox browser for Web administration or Web client

e. Accessories available for turnkey offering

Team on the Run comes as Software as a Service (SaaS) and works on mobile devices such as smartphones, tablets and PCs. In addition, Team on the Run works with several device and accessory providers such as Samsung, Sonim, Kyocera providing its services on ruggedized devices, tablets etc. Team on the Run also has integrates with multiple accessories to enhance the push-to-talk service with RSM and emergency buttons:

- Pryme BT-PTT-Z MINI
- Aina wireless RSM – PTT
- Aina wireless button for emergency
- Klein Valor RSM
- Rexon BT-24HC
- Savox SH-01
- Stone Mountain Phoenix

- Savox
- Klein Drift PTT Earpiece
- Klein Triumph 1-Wire

Compatibility with Android and iOS devices can be provided upon request.

- f. Thoroughness of the vetting process used to select partners
A thorough industry analysis and full RFP process were used to select StreamWIDE as UScellular's solution provider. StreamWIDE has been recognized among the players within the industry being an expert in carrier-grade telecom solutions serving 130+operators, 100M+ End-Users worldwide with live operations in 71 countries / 5 continents.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
The solution has been tested in both UScellular and StreamWIDE labs for integration with related UScellular solutions, such as UScellular provided mobile devices (Android and IOS smartphones, tablets etc.). The solution is in use both internally and deployed with many UScellular customers.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
Team on the Run installation will be supported by StreamWIDE and UScellular teams. The following are important elements to work before the solution is deployed
- Understand the customer problem
 - Define how Team on the Run will contribute to the solution of problem
 - Identify use cases and user roles (admin, dispatcher, users)
 - Identify the need of accessories
 - Gather user phone numbers to configure and device types (Android / iPhone)

UScellular is will deliver the devices. StreamWIDE will deploy the Team on the Run solution.

- b. Project coordination
Team on the Run project coordination will be performed by StreamWIDE and UScellular teams. A limited duration trial of the solution can be coordinated as needed. All StreamWIDE project coordination is done remotely for accounts 500 users or less.
- c. Installation and Testing process
Based on the identified user list and use cases Team on the Run team will support the initial setup to maximize the value captured by customer:
- Creation of users
 - Configuration of user rights and roles
 - Process template creation (1 template and 1-hour consultation included)
 - Activation of devices
 - Assistance with implementation questions

- d. Client Infrastructure and support assessment process

Our dedicated support team will work with you to understand your infrastructure and assess your support needs. We will create a comprehensive support plan to meet those needs.

- e. End user Acceptance process

Once installation and deployment are complete StreamWIDE will conduct training and in this session the acceptance is reached. At this point, the customer can reach Team on the Run support.

- f. Approach to maintenance and support

StreamWIDE customers have access to 24/7 email support. The contact button on the client app links you to the support team.

- g. Initial and Ongoing Training provided

Team on the Run training is performed by StreamWIDE team product expert and typically delivered remotely. The training is centered on the customer use cases.

Ongoing questions on the product after initial training can be addressed by the Team on the Run support team.

- h. On-going support and enhancement over the life of the agreement

The Team on the Run Account Manager is responsible for customer satisfaction and the single point of contact for commercial requests such as additional licenses or plan changes.

Team on the Run is an active product and it continuously evolves. Feature enhancements are pushed via the SaaS platform to customers. Our marketing team communicates the enhancements and our support and account managers are ready to answer any questions. Typically, enhancements in existing features are backward compatible so minimum impact is expected on customers already using the functions.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution

Team on the Run standard implementation includes the following services provided by StreamWIDE:

- Implementation services / My Business activation
 - o One-hour consultation and one custom process/form template
 - o Initial configuration and creation of users on SaaS solution
 - o Installation support of mobile client app on customer devices
 - o Training session
- Team on the Run SaaS Service
- Team on the Run Support service

Additional consulting services can be ordered as needed.

- b. Experience and qualifications of partners and subcontractors
StreamWIDE implementation and support engineers are full time and specialized in the Team on the Run product. Internal processes in place allow escalation to product and development managers as questions or issues require.
- c. Description of Additional Integration and Consulting Services provided
Additionally, StreamWIDE can provide consultation services for
 - Creation of custom processes/ forms on My Business
 - Special Integration services (API integration with external systems)
 - Additional cloud storage may apply for My business form data



StreamWIDE

Warning Procedure for Internal and External Customers

Operational Guideline

Document History:

Version #	Date	Edition cause	Author(s)
1.0	16/04/2012	First Release	Victorita ANECHITEI

Document Approvals:

Version #	Date	Name	Visa
1.0	16/04/2012	Zakaria NADHIR	ZN

Storage :

PDF Document	Document Sources
Alfresco:\Quality\05.Process&Procedures\Technical Support	Alfresco:\Quality\04.Sources\Technical Support

TABLE OF CONTENTS

1.	Introduction	4
1.1.	Purpose	4
1.2.	Scope	4
1.3.	Definitions and Acronyms	4
1.4.	Role	4
2.	Inputs.....	4
3.	Activities	4
3.1.	On the CTO's side	4
3.1.1.	Gathering and analyzing information	4
3.1.2.	E-mail to Support and Quality	4
3.2.	On the Support Manager's side.....	5
3.2.1.	Warning e-mail internally	5
3.2.1.	Warning e-mail for customers.....	5
3.3.	On the Customer's side	5

1. Introduction

1.1. Purpose

This document describes the policy implemented by StreamWide to insure a proactive support attitude in the case of redundant critical issues and a better circuit of pertinent information inside StreamWide regarding service impacting issues.

1.2. Scope

This procedure relates to the full range of company activities, mainly to issues regarding software development, delivery and technical support.

1.3. Definitions and Acronyms

CTO – Chief Technology Officer

1.4. Role

Under this procedure the CTO is in charge of selecting the pertinent warnings to be sent internally and to the customers.

2. Inputs

Feedback from support, delivery and product teams on critical issues.

3. Activities

3.1. On the CTO's side

3.1.1. Gathering and analyzing information

Every week, the CTO (Zakaria Nadhir) will analyze the main problematic issues that will appear on the customers platforms based on feedback from delivery, support and product teams. He will decide whether there is a real need to send a warning internally and to the customers. The CTO is in charge of selecting the most risky issues among the ones that have been escalated in the given period of time.

3.1.2. E-mail to Support and Quality

As often as needed, the CTO will send an e-mail to the Support and Quality departments to inform them of the main problems that have occurred during the given period and that might risk reappearing on other platforms.

The e-mail sent by the CTO will include for each issue raised:

- a description of the issue

© StreamWIDE	Author: vanechitei	
All rights reserved	sw_OG_Warning Procedure for Internal and External Customers10	4/5

- which are the versions of products that might be impacted
- which are the exceptions to be taken into account when sending the warning e-mails to the customers.

3.2. On the Support Manager's side

3.2.1. Warning e-mail internally

Based on the CTO's e-mail, the support manager must issue a warning e-mail internally with the following list of users, all in Cci:

- support team
- delivery team
- product teams (PMs)
- sales.

Each support engineer has under his direct supervision a list of customers. (See **StreamWIDE Support - Internal Handover Process**, on **Alfreco:\Quality\05.Process&Procedures\Technical Support**). Each of them will have to check in the CRM to see which of his/her customers/platforms might be impacted by the issues raised in the Support Managers' e-mail. If any identified customers, they will inform the Support Manager about it.

This task is considered as level 1 Task, on the support list of tasks.

3.2.1. Warning e-mail for customers

In three days time after having received the CTO's e-mail, the Support Manager will have to send a warning e-mail to all customers concerned by the issues. A special e-mail template will be used for the warning and each customer will receive an individual e-mail (no Cci). Each sent e-mail will be accompanied by the opening of a ticket in the ticketing tool.

- Prior to issuing a warning to customer, Support should inform sales that a warning will be issued. If sales do not answer within 2 workdays, warning is issued, if they ask not to issue or to delay the warning for commercial reasons, they take the responsibility if any problem related to the warning occurs on the platforms. Information to sales should include the solutions they can propose to their customers.
- When the warning is issued to a customer it should contain also a solution/recommendation. A warning with no solution proposed would generate high customer anxiety and may trigger wrong reactions.

3.3. On the Customer's side

Based on the raised issue, the customer should get in touch with his Sales contact inside of StreamWide to be informed of the options that we might propose to fix the issue (e.g. : ask for an upgrade, a fix etc.)

If the customer doesn't reply after two reminders, the Support department is allowed to close the ticket and consider the warning closed.

© StreamWIDE	Author: vanechitei	
All rights reserved	sw_OG_Warning Procedure for Internal and External Customers10	5/5



StreamWIDE Security 1.0



STREAMWIDE Information Security Management System

Product Document



StreamWIDE Security 1.0

Product Document

Document History:

Version #	Date	Edition cause	Author(s)
1.0	2020-Feb-10	First release	Cosmin CECANAU

Document Approvals:

Version #	Date	Name	Visa
1.0	2020-Feb-10	Zakaria NADHIR	CTO

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	2/19



StreamWIDE Security 1.0

Product Document

TABLE OF CONTENTS

1.General view	4
2.Direction	5
3.Scope	6
4.Top Management Leadership and Commitment	7
5.Internal Audit and Employees Continuous Mindset Growth	8
6.Infrastructure Continuous Security	9
7.Software Continuous Security	10
7.1.IDE: IntelliJ IDEA SonarLint	10
7.2.Version Control System: Subversion	11
7.3.Manual Security Check	12
7.3.1.Team Leader Review	12
7.3.2.Dedicated Testing Team	12
7.4.Automated Security Scan	12
7.4.1.Sonar Qube	14
7.4.2.Lint	16
7.4.3.Mobile Security Framework (MobSF)	18

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	3/19



StreamWIDE Security 1.0

Product Document

1. General view

An Information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data.

The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	4/19



StreamWIDE Security 1.0

Product Document

2. Direction

StreamWIDE guidelines and provisions for establishing, implementing, maintaining and continually improving the internal ISMS are following **ISO/IEC 27001:2013** recommendations.

ISO 27001 is a specification for creating an ISMS. It does not mandate specific actions, but includes suggestions for documentation, internal audits, continual improvement, and corrective and preventive action.

StreamWIDE Top Management and Security Team are doing best efforts to follow and adapt the standard recommendations with the goal of keeping our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	5/19



StreamWIDE Security 1.0

Product Document

3. Scope

The document offers a high level overview over the *concrete and provable* actions taken by the Company in order to ensure continuous security improvements

- Top Management Leadership and Commitment
- Internal Audits and Employees Continuous Mindset Growth
- Infrastructure Continuous Security
- Software Continuous Security

External references should be additionally provided:

- [SW_InternalSecurityPolicy](#) - Internal Security Policy document
- [SW_0G_BusinessContinuityPlan](#) - Business Continuity Plan document

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	6/19



4. Top Management Leadership and Commitment

Top Management assume their responsibilities for Information Security/Business Continuity and ensure all required actions are part of company strategy.

Business Continuity Process

The STREAMWIDE Business Continuity Plan aims to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters include all the cases where business is not able to occur under normal conditions.

The main objectives of the plan are:

- Facilitate effective decision-making to ensure that StreamWIDE operations are restored in timely manner in case of service interruption
- Protect essential facilities, equipment, vital records and other assets
- Protect the well-being of StreamWIDE's employees and customers
- Minimize loss of revenue/customers
- Maintain public image and reputation
- Minimize loss of data
- Minimize the critical decisions to be made in a time of crisis
- Identify teams which would need to respond to a crisis

The process is described in [sw_0G_BusinessContinuityPlan](#) document.

Management follow up and review

The main company security objectives are reviewed each week during the official Masterplan Status Meeting with Product Managers.

Additionally, relevant KPIs on [Software Security](#) are sent weekly for management reviews.

Among other information they include the number of vulnerabilities and bugs reported when scanning the code using tools recommended by OWASP.

Security Events Reporting

Since executives are the ones who have the most influence in an organization, Security objectives or Measures for Crisis management are always part of Top Management communication.

Internal Security Policy

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, Top Management has implemented a number of security measures presented by [SW_InternalSecurityPolicy](#).

With this policy, STREAMWIDE ensures that we gather, store and handle data fairly, transparently and with respect towards individual rights.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	7/19



5. Internal Audit and Employees Continuous Mindset Growth

STREAMWIDE Internal security audits are oriented to people awareness, processes, policies and infrastructure hardening.

Software Audit is treated as independent process using automated solutions according to Continuous Security guidelines.

Auditors

Internal audits are performed and coordinated by employees with **important company history and relevant experience in various domains (development, linux administration, team lead, team management)**.

Cosmin CECANAU

Position: Product Manager Installer Team, Manager of Romania Security department, certified for Internal Auditor iso 27001/2013 international recognition

Activity: Coordinates the security department activities based on priorities (implementations, standards appliance, trainings)

Studied: The Faculty of Automatic Control and Computer Science (Polytechnic University of Bucharest);
In StreamWIDE since 2006 ,

Thomas BOUTON

Position: Chief Software Architect / Chief Security Officer

Activity: Coordinates company security activities according to customers needs, creates and validates software architectures.

Studied : Ecole Nationale Supérieure des Télécommunications de Paris
In StreamWIDE since 2001,

Cristian RADU

Position: Product Manager StreamWIDE Messaging System & SmartMS Backend

Activity: Collaborates with the security department bringing concrete lessons learned, real usecases and needs from Messaging Product life history & SmartMS backend new challenges.

Studied: The Faculty of Electronics Telecommunications and Information Technology (Polytechnic University Bucharest);
In StreamWIDE since 2008,

Scheduling

The frequency for Internal auditing a StreamWIDE Subsidiary depends on the activities performed and the number of employees. It is done once or twice per year.

Normally the audit is done on-site. But depending on situation can be done remotely. The audit lasts *3 to 5 days*.

Reporting and Follow Up

The internal Audit is finished by a "conclusions meeting" with the local management. Also an email with conclusions and action plan is sent to the Top Management.

The actions will be followed up weekly as explained in the "Top Management Leadership and Commitment" chapter.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	8/19



6. Infrastructure Continuous Security

Identifying vulnerabilities and gaining visibility into the number of smart devices and their role within the infrastructure can help reduce the risk of a successful cyberattack.

It's important to keep a detailed inventory of all IoTs, constantly check for new security updates that address known vulnerabilities, and maintain them on a segregated network that's completely isolated from other critical systems.

Actions for increasing the security of the company infrastructure are decided during regular audits or during technical workshops.

Some element are listed below, but for confidentiality reasons there are no concrete technical descriptions for the actions taken.

Network Topology

Keeping up-to-date and understanding our own topological structure of the network, physically or logically it is a key requirement for our administrators.

Network segmentation

Network segmentation is a mandatory element for ensuring security.

VPN

VPN solution having high level encryption and Multi Factor Authentication is a mandatory element to ensure safe remote connections.

Firewall

Firewall is one of the cornerstones of any network security strategy so it is mandatory to use a performant solution.

Backup

Ensuring backups gives fast recovery in case of data loss.

Wifi

Wifi Security hardening has also been taken in consideration.

External Scan

External scanning is regularly notifying the administrators about potential flaws of our network.

Intrusion Detection

Intrusion detection systems or traps are offering precious time in preventing a cyberattack.

Secure Communication

Replacing deprecated protocols with latest secure protocols is also a continuous process.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	9/19



StreamWIDE Security 1.0

Product Document

7. Software Continuous Security

StreamWIDE target is to align all proprietary software modules/applications to the newest recommendations regarding Continuous Security.

This chapter explains the process used to ensure Continuous Security for an Android Mobile Application belonging to StreamWIDE software suite.

The rest of **STREAMWIDE** software modules/applications implement **PARTIALLY** this model at this time.

 Code inspection starts from the very first code view due to specialized IDE.

 A popular version control system is used to ensure that all the changes are tracked or can be reverted.

 Manual checking and testing is done by Team Leaders and dedicated Testing Team.

 Automated scan is done by popular and powerful tools on daily, on demand or on commit basis in order to help the team with comprehensive security reports or regressions alerts.

7.1. IDE: IntelliJ IDEA SonarLint

StreamWIDE Android team uses **IntelliJ IDEA with SonarLint plugin** for code development.

IntelliJ IDEA is a Java integrated development environment (IDE) for developing computer software.

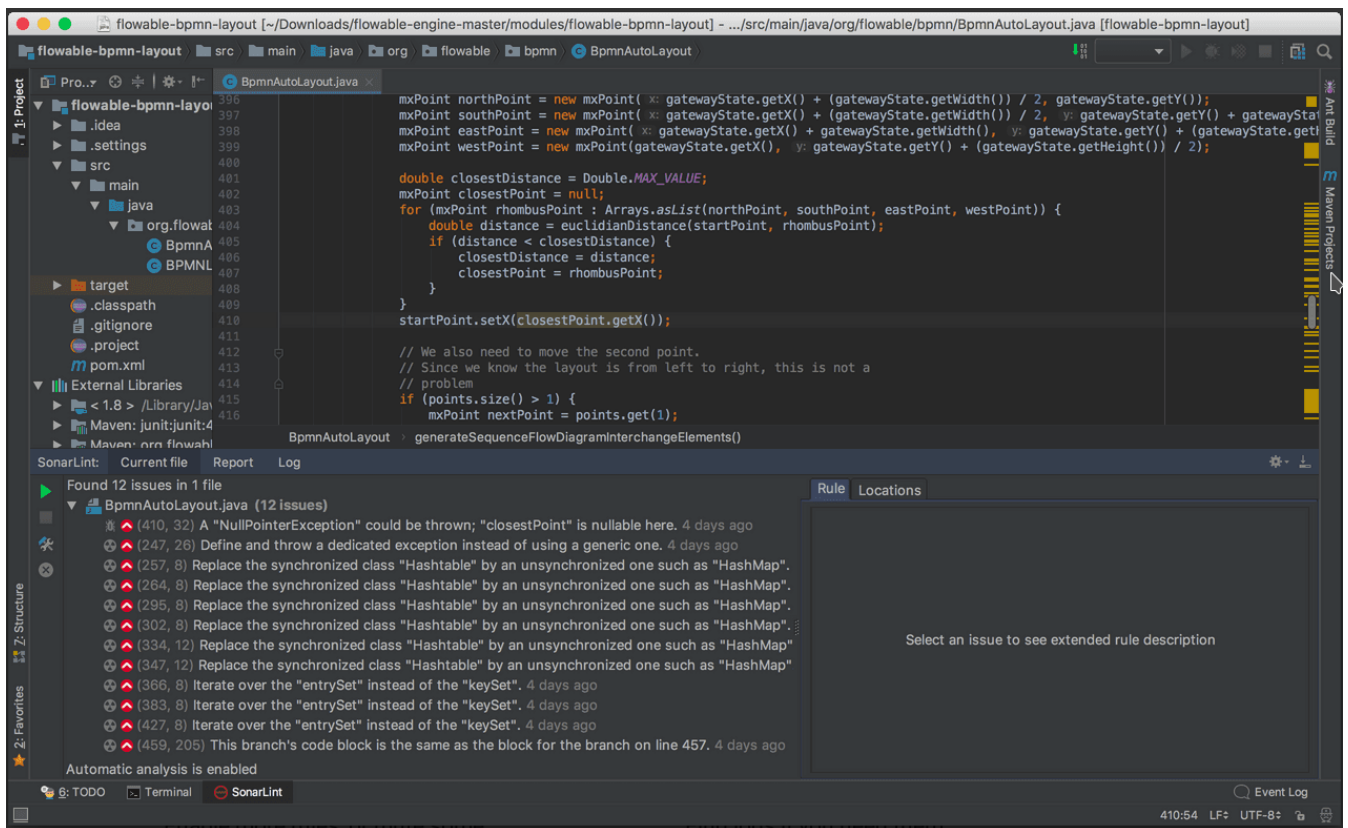
SonarLint is an IDE extension that helps detecting and fixing quality issues as code is being written. Like a spell checker, SonarLint squiggles flaws so that they can be fixed before committing code.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	10/19



StreamWIDE Security 1.0

Product Document



7.2. Version Control System: Subversion

Android Team uses **Subversion** in order to keep the track of every code modification.

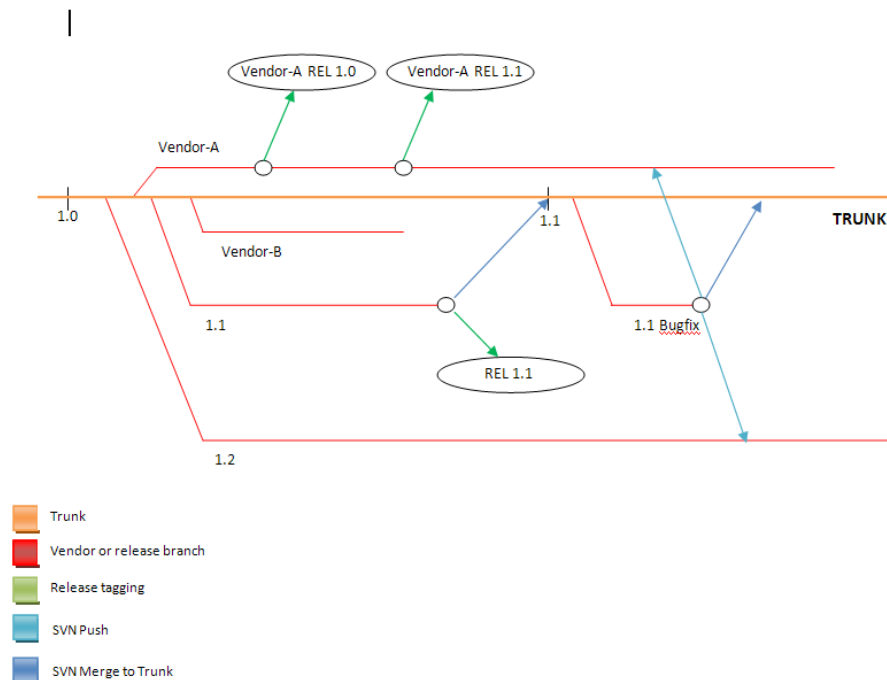


Subversion is a free/open source version control system. That is, Subversion manages files and directories, and the changes made to them, over time.

This allows us to recover older versions of the data or examine the history of how your data changed.

Android Team is using the recommended mechanism with trunk & branches.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	11/19



7.3. Manual Security Check

7.3.1. Team Leader Review

The Android development team distribution ensures a tight control for every piece of code which reaches the repository.

The team is split in small subteams lead by Team Leaders.

Any new code is reviewed by at least a Team Leader before being merged to the main Subversion branch.

Critical code is also reviewed by Product Manager.

7.3.2. Dedicated Testing Team

A dedicated testing team is in-charged of manual testing every new minor and major release.

Although the tests are mostly functional, security fixes receive a special attention and important time allocated.

7.4. Automated Security Scan

A complex mechanism is designed to ensure security scanning on a regular base or on each merge in the main branch (depending on the configuration).

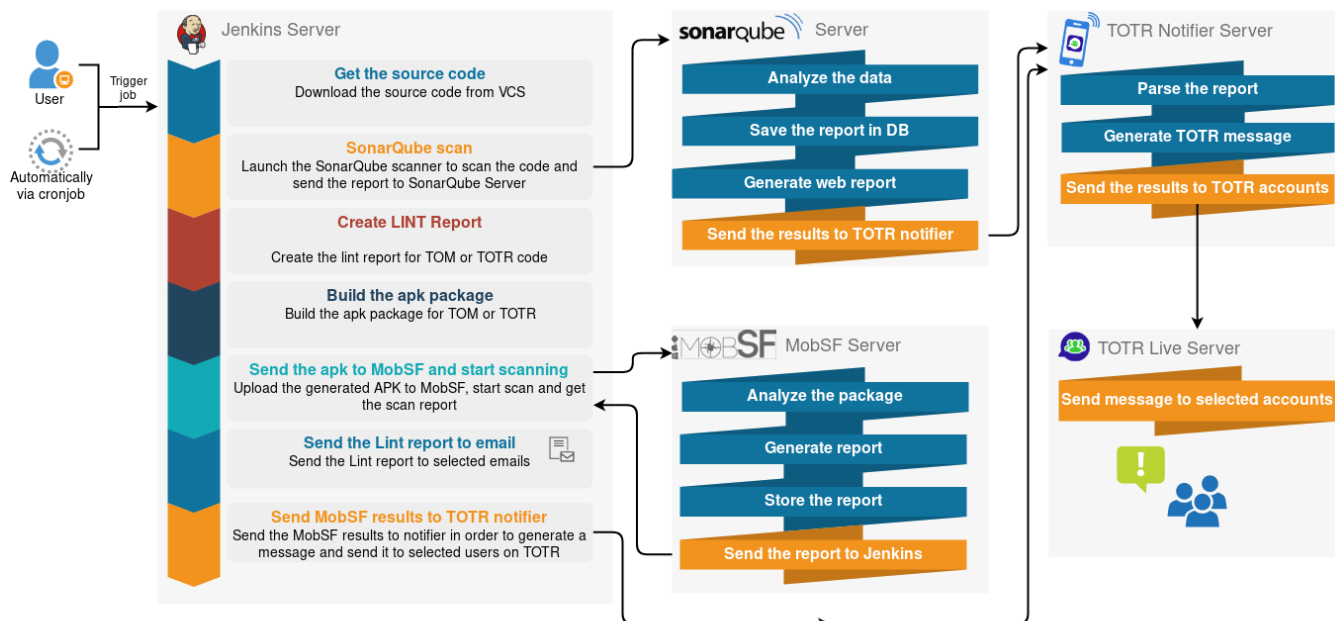
Powerful tools like Jenkins, SonarQube, Lint or MobSF are combined to ensure a complete security verification as it is presented in the diagram below.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	12/19



StreamWIDE Security 1.0

Product Document



© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	13/19

7.4.1. Sonar Qube



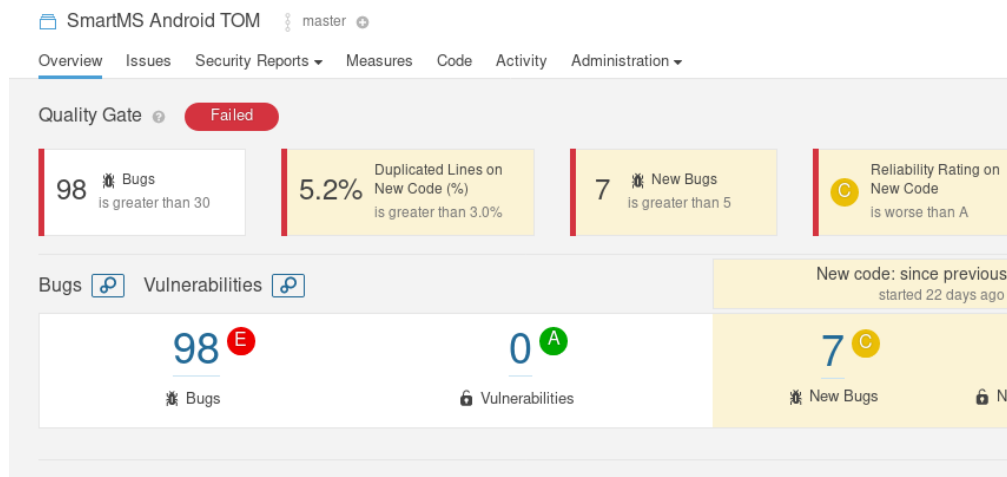
The OWASP SonarQube project aims to provide open source Static Application Security Testing (SAST) using the existing open source solutions.

SonarQube is one of the world's most popular continuous code quality tools and it's actively used by many developers and companies.

SonarQube has helped Android team to improve drastically the quality of the software.

Daily reports are showing the potential vulnerabilities and issues helping the team to understand the threats and principles for good quality and security.

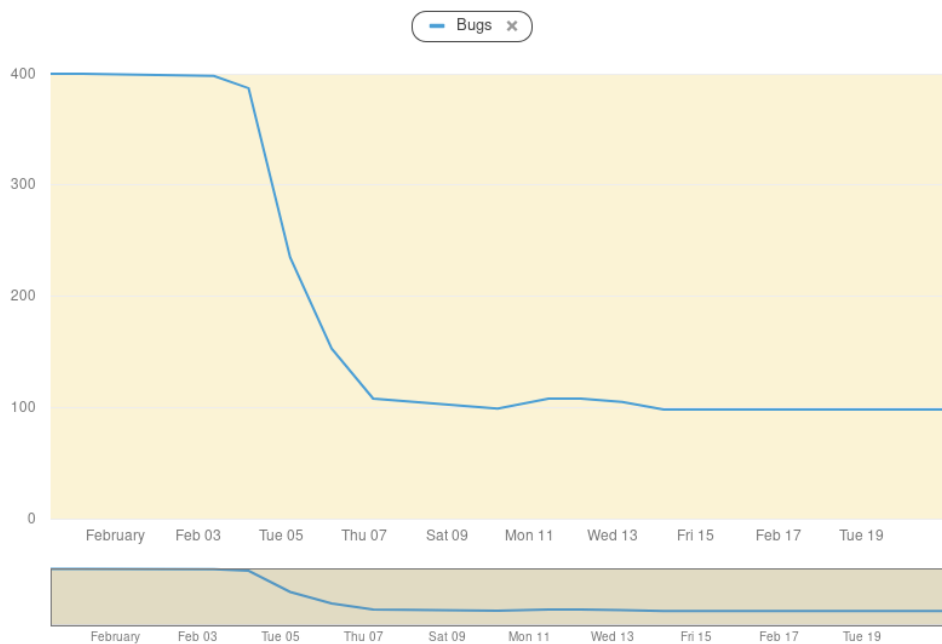
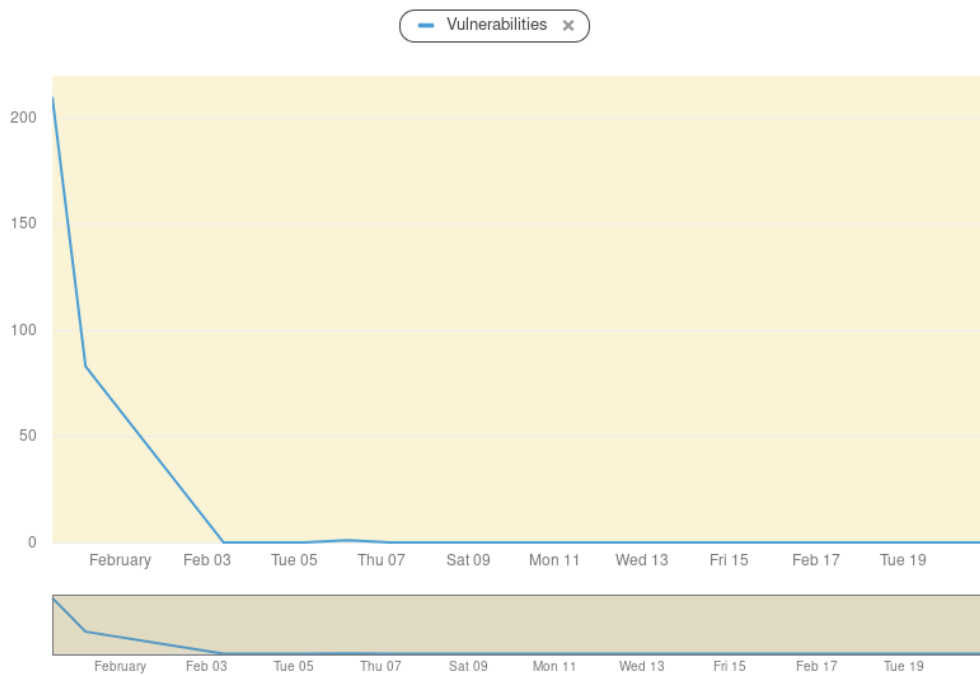
The reports below are taken at 22 Feb 2019. By this date the team has done big efforts to decrease to 0 the number of vulnerabilities and it is concentrating right now to decrease also the number of potential bugs.





StreamWIDE Security 1.0

Product Document



© StreamWIDE All rights reserved	Author: Cosmin CECANAU StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	Date: 2019-Feb-10 15/19



StreamWIDE Security 1.0

Product Document

7.4.2. Lint

Android build system provides a lot of tools to optimize the code, find potential issues, improve performance, etc. One of the tool it supports is Lint. Lint is a tool which analyzes the source code and flags potential bugs and errors during the build.

Daily reports are showing the potential vulnerabilities and issues helping the team to understand the threats and principles for good quality and security.

The reports below are taken at 22 Feb 2019. By this date the team has done big efforts to decrease the number of vulnerability notices and it is concentrating right now to decrease also the number of potential issues..

Overview

Correctness	
4	! MissingRegistered : Missing registered class
9	! ApplySharedPref : Use apply() on SharedPreferences
1	! PrivateApi : Using Private APIs
1	! UnusedAttribute : Attribute unused on older versions
1	! BatteryLife : Battery Life Issues
5	! InflateParams : Layout Inflation without a Parent
1	! NewerVersionAvailable : Newer Library Versions Available
5	! RestrictedApi : Restricted API
54	! SwitchIntDef : Missing @IntDef in Switch
Correctness:Messages	
3	! Typos : Spelling error
Security	
1	! BadHostnameVerifier : Insecure HostnameVerifier
3	! HardwareIds : Hardware Id Usage
1	! SetJavaScriptEnabled : Using setJavaScriptEnabled

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	16/19



StreamWIDE Security 1.0

Product Document

Performance

2	⚠ DrawAllocation : Memory allocations within drawing code
2	⚠ WakelockTimeout : Using wakeLock without timeout
6	⚠ ObsoleteLayoutParam : Obsolete layout params
73	⚠ ObsoleteSdkInt : Obsolete SDK_INT Version Check
3	⚠ StaticFieldLeak : Static Field Leaks
1	⚠ VectorPath : Long vector paths
4	⚠ UseSparseArrays : HashMap can be replaced with SparseArray
1	⚠ DisableBaselineAlignment : Missing baselineAligned attribute
2	⚠ InefficientWeight : Inefficient layout weight
6	⚠ Overdraw : Overdraw: Painting regions more than once
82	⚠ UnusedResources : Unused resources
5	⚠ UselessParent : Useless parent layout
35	⚠ UnusedIds : Unused id
1	⚠ UnusedNamespace : Unused namespace

Usability:Typography

1	⚠ TypographyQuotes : Straight quotes can be replaced with curvy quotes

7.4.3. Mobile Security Framework (MobSF)

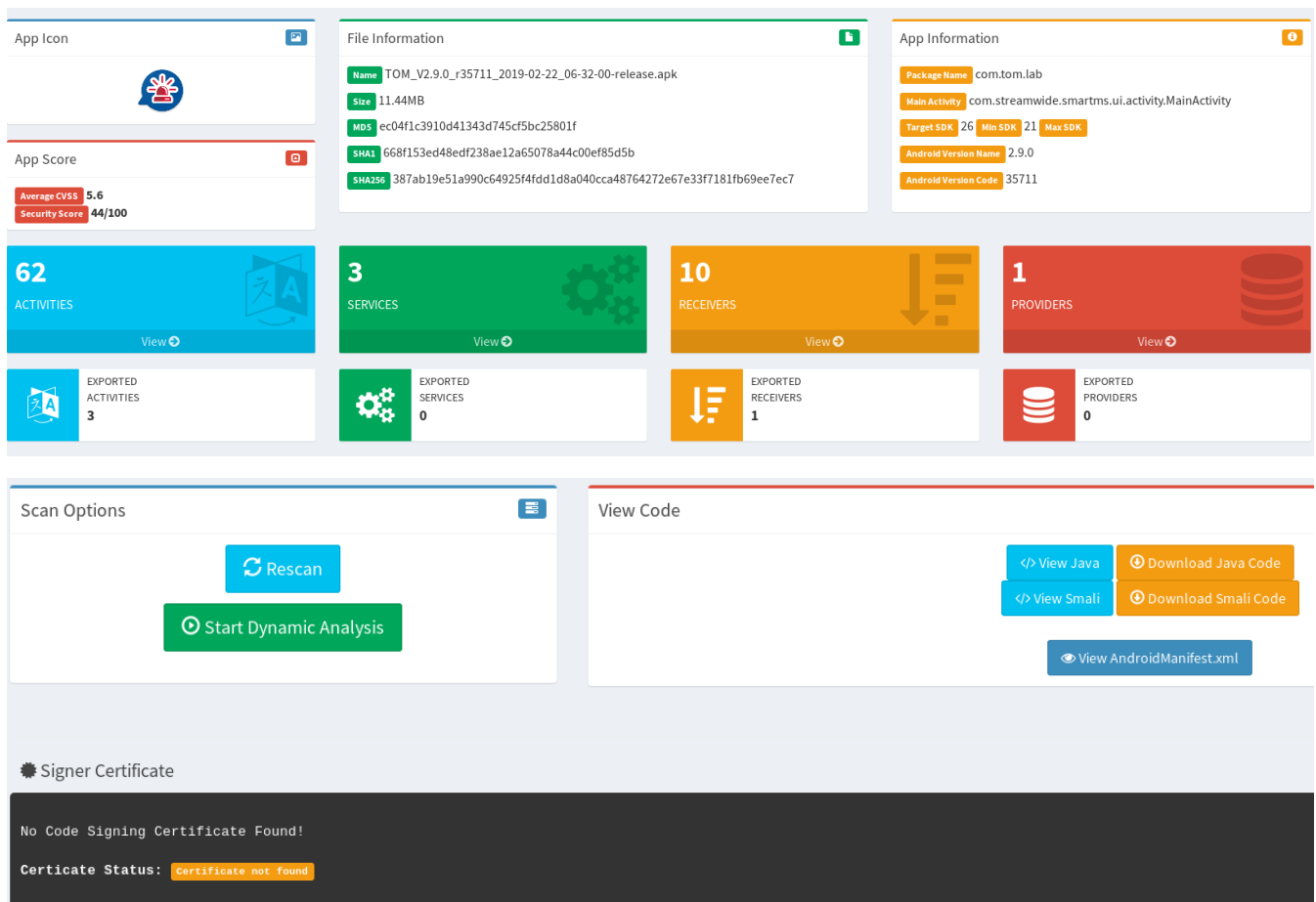


Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing framework capable of performing static, dynamic and malware analysis. It can be used for effective and fast security analysis of Android, iOS and Windows mobile applications and support both binaries (APK, IPA & APPX) and zipped source code.

MobSF can do dynamic application testing at runtime for Android apps.

This option it is used by Android Team on a regular basis to investigate the potential security issues of the apk.

Below are some examples of report taken on 22 Feb 2019.



The screenshot displays the MobSF web interface with the following sections:

- App Icon:** Shows the application icon for 'com.tom.lab'.
- App Score:** Displays an Average CVSS of 5.6 and a Security Score of 44/100.
- File Information:**
 - Name: TOM_V2.9.0_r35711_2019-02-22_06-32-00-release.apk
 - Size: 11.44MB
 - MD5: ec04f1c3910d41343d745cf5bc25801f
 - SHA1: 668f153ed48edf238ae12a65078a44c00ef85d5b
 - SHA256: 387ab19e51a990c64925f4fdd1d8a040cca48764272e67e33f7181fb69ee7ec7
- App Information:**
 - Package Name: com.tom.lab
 - Main Activity: com.streamwide.smartms.ui.activity.MainActivity
 - Target SDK: 26, Min SDK: 21, Max SDK: 28
 - Android Version Name: 2.9.0
 - Android Version Code: 35711
- Summary Cards:**
 - 62 ACTIVITIES (View)
 - 3 SERVICES (View)
 - 10 RECEIVERS (View)
 - 1 PROVIDERS (View)
- Exported Data:**
 - EXPORTED ACTIVITIES: 3
 - EXPORTED SERVICES: 0
 - EXPORTED RECEIVERS: 1
 - EXPORTED PROVIDERS: 0
- Scan Options:**
 - Rescan button
 - Start Dynamic Analysis button
- View Code:**
 - View Java / Download Java Code
 - View Smali / Download Smali Code
 - View AndroidManifest.xml
- Signer Certificate:**
 - No Code Signing Certificate Found!
 - Certificate Status: Certificate not found



StreamWIDE Security 1.0

Product Document

Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	dangerous	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points an networks.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	19/19



StreamWIDE

Security - Internal Policy

Product Document



StreamWIDE Security 1.0

Product Document

Document History:

Version #	Date	Edition cause	Author(s)
1.0	2019-Feb-10	First release	Cosmin CECANAU

Document Approvals:

Version #	Date	Name	Visa
1.0	2019-Feb-10	Cosmin CECANAU	Security Manager

TABLE OF CONTENTS

1. Policy brief & purpose	4
2. Scope	5
3. Policy elements	6
3.1. Confidential data	6
3.2. Protect personal and company devices	6
3.3. Keep emails safe	7
3.4. Manage passwords properly	7
3.5. Transfer data securely	7
3.6. Additional measures	8
3.7. Social media policy	8
3.8. Internet usage policy	9
3.9. Remote employees	9
4. Disciplinary Action	11
4.1. Take security seriously	11



1. Policy brief & purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

It refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	4/11



2. Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	5/11

3. Policy elements

3.1. Confidential data

Confidential data is secret and valuable.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive customer data.)
- Constitute the backbone of our business, giving us a competitive advantage

Employees will unavoidably receive and handle personal and private information about clients, partners and our company. We want to make sure that this information is well-protected.

Our company most important confidential assets are:

- In-house developed software
- Unpublished financial information
- Data of Customers/Partners/Vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Each employee is obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

3.2. Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only. We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	6/11

When new hires receive company-issued equipment they will receive instructions for:

- *Disk encryption setup*
- *Password management tool setup*
- *Installation of antivirus/ anti-malware software*

They should follow instructions to protect their devices and refer to our *Internal Support Engineers/ Network Engineers* if they have any questions.

3.3. Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Do not open emails when sender is unknown. Even when sender is known, it may be a fake origin (spoofing). In such cases be cautious if the title or content looks unusual for such sender.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they can refer to our *IT Support department*.

3.4. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every three months.

3.5. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our *Internal Support Engineers* for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	7/11

connection.

- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our *IT Specialists/ Network Engineers* need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our *IT Specialists/ Network Engineers* must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Internal Support engineers are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

3.6. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to *HR/ IT Department*.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy (as described in the corresponding chapters below).

Our *Internal Support Engineers/ Network Administrators* will:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company does all the efforts to have all physical and digital shields to protect information.

3.7. Social media policy

Social media refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them.

We allow employees to access their personal accounts at work. But, we expect them to act responsibly and ensure their productivity isn't affected. Using social media excessively while at work can reduce efficiency and concentration. Whether employees are using their accounts for business or personal purposes, they may easily get sidetracked by the vast amount of available content.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	8/11

We advise our employees to:

- Use their common sense. If employees neglect their job duties to spend time on social media, their decline in productivity will show on their performance reviews.
- Ensure others know that personal account or statements don't represent our company. Employees shouldn't state or imply that their personal opinions and content are authorized or endorsed by our company. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
- Avoid sharing intellectual property like trademarks on a personal account without approval. Confidentiality policies and laws always apply.
- Avoid any defamatory, offensive or derogatory content. It may be considered as a violation of our company's anti-harassment policy, if directed towards colleagues, clients or partners.

3.8. Internet usage policy

Our employees are advised to use our company's internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor.

3.9. Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	9/11



StreamWIDE Security 1.0

Product Document

accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our *Internal Support Engineers/ IT Administrators*.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	10/11

4. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary actions up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face Progressive Discipline, even if their behavior hasn't resulted in a security breach.

Our Progressive Discipline policy outlines the steps we will take to address an employee's misconduct.

We recognize that people make mistakes and our employees may not always follow our policies closely. We want to give our employees a chance to correct their behavior when possible and assist them in the process. We also want to ensure that serious offenses are thoroughly investigated and dealt with.

This policy applies to all our employees.

Our disciplinary process has six steps of increasing strictness. These steps are:

- Verbal warning
- Informal meeting with supervisor
- Formal reprimand
- Formal disciplinary meeting
- Penalties
- Termination

4.1. Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Appendix M

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory D, E, and F: Field Service Management, Workforce Management, and Mobile Data Collection / Mobile Forms

Effort +



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
Effort+ - An acronym that stands for "Effortless Field Force Optimization and Reporting Tool"
- b. General Application Area
Subcategories D, E, and F
- c. General capabilities provided
Capabilities include:
 - Dynamic Mobile Form engine, to define and capture data.
 - Offline Mobile data collection App for IOS & Android.
 - Flexibility to Capture different data types such as images, videos, and audio along with signature.
 - Geotagging of activities to ensure activities were performed on-premise.
 - Route optimization to ensure maximum coverage.
 - Workflow automation to take care of approvals and exceptions, that allow for data to flow to necessary people for action (all through mobile apps).
- d. Expected impact on cost/performance/functionality, etc.
 - World over FSM and Workforce management has been a key challenge and organizations have deployed solutions that are heavy and expensive.
 - Effort+ ensures that the deployment is hassle-free, economical and scalable all through a cloud-based platform, secure storage and dynamic mobile application.
 - Experience and studies have proven that cost savings of minimum 35% is achieved when organizations choose to deploy Effort+.
- e. Subcontractors/partners involved in delivering service
Goldie Group is a regional partner with Spoors the brand owner of Effort+. We will be serving and servicing the Workforce, FSM and Mobile data collection needs of the client along with Spoors team.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described

Our tool provides:

- A dynamic form builder with 30+ data types that allows for quickly building and deploying mobile forms that can be used by field personnel to both record and collect data.
- Flexible and easy workflows that allow for approvals and sanctions on the fly with managers and subordinates working their way through the mobile app that serves them the necessary data.
- Cloud-based service - no worry on infrastructure downtime or scalability.
- Offline data collection along with Geo-stamps ensure veracity of data!
- Ability to create 1000s of forms on the go using a dynamic dashboard that also serves as a single window to provide comprehensive views of activities and data flow.

- b. Applicability to government needs

The solution is dynamic and domain-agnostic. Hence can be applied to any governmental needs. In fact, some of the local government in Indian region have used it to collect data of farmers, distribution of subsidies, etc.

Caters to all the governmental protocols and procedures ensuring data privacy and security.

- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.

Provide references

500+ global customers from various domains including Siemens, AtoS Switzerland, HomeCredit, Truemoney, L&T and other big names.

- d. Overall interoperability of turnkey system for government use

The solution is a data definition and collection tool. Works with a simple database that allows for data to flow to different systems through custom APIs.

- e. Accessories available for turnkey offering

N/A

- f. Thoroughness of the vetting process used to select partners

Goldie Group selects and offers solutions that are robust and proven in the market. We work to ensure our 30-year legacy is not compromised.

- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

Client partners usually do integration tests as appropriate to suit their needs.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
 - Goldie Group and Spoors team will work towards initial form and workflow development as needed.
 - Will ensure that sanity and acceptance is done for forms and work flow deployments.
 - A Business Analysts will be available long-term for consultation at cost (USD \$75 per man hour).
- b. Project coordination
 - Goldie group will project manage all the operations and deliverables with all the involved parties and the client partners.
- c. Installation and Testing process
 - Initial form definitions, creation and deployment will be done by Goldie Group.
 - Field tests can be done in conjunction with client teams along with Goldie Group's involvement.
 - Once the acceptance is signed off mass roll out will be ensured by Goldie Group team to the necessary devices/personnel.
- d. Client Infrastructure and support assessment process
 - Our systems are all cloud-based and assessment if need be can be performed by the client partners.
 - We do regular security audits to ensure there is no data leakage or security breach (with third party assessments both for platform and the mobile applications). PEN (Penetration) tests are performed for checking security breaches, on a periodic basis.
- e. End user Acceptance process
 - Goldie will work with client partner to define the final acceptance document.
 - Goldie will work with client teams to sign-off on all of the agreed terms before mass roll out.
- f. Approach to maintenance and support
 - Cloud-based systems are generally taken care of by Goldie's partners and hence uptime and availability are ensured to 99.99% basis cloud service providers.
 - SLAs and insurances can be provided as a separate document should there be a need.
- g. Initial and Ongoing Training provided
 - Initial hand holding will be done, and device deployments will be assisted.
 - Ongoing training for new features are conducted on a regular basis.
 - Ongoing support can be purchased, and our BA (Business Analysts) will work remotely or on-prem to hand hold the teams. Incidentals, travel, boarding during on-prem visits will be borne by the clients.
- h. On-going support and enhancement over the life of the agreement
 - Free updates and feature inclusions are covered as part of the license agreement.
 - Support is included in the licensing cost. On-prem support is chargeable.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
Separate document on SLAs will be shared on a need basis once we are onboard with client partners. This shall detail availability, uptime, and other insurance measures to ensure smooth business operations.
- b. Experience and qualifications of partners and subcontractors
Goldie Group celebrates a 30+ year experience and knowhow in operations, warehousing, distribution and servicing technology needs for clients. Spoors is a young and dynamic solution company with more than 8 years of experience and several man years of technical know-how. The dynamic duo shall ensure our clients succeed even during tough times like the current pandemic.
- c. Description of Additional Integration and Consulting Services provided
 - On a need basis Goldie Group shall develop custom software and solutions that are required to augment the current business operations of the client
 - Our current supply chain platforms and back end integrations will also come in use for the large-scale deployment in disparate geographies.

Scalefusion MDM: Unified Device & Endpoint Management Solution

Terms of Service

Version: 4.0

Effective Date: 1 February, 2020

This “**Scalefusion (formerly MobiLock Pro)**” Terms of Service Agreement (the “Agreement”) is between you and ProMobi Technologies Pvt Ltd (India - U74900PN2014PTC150210) (“ProMobi”). If you are agreeing to this Agreement not as an individual but on behalf of your company, then “Customer” or “you” means your company, and you are binding your company to this Agreement. ProMobi may modify this Agreement from time to time, subject to the terms in Section 16.7 (Changes to this Agreement) below.

By clicking on the “I agree” (or similar button/link/checkbox) that is presented to you at the time of your Order, or by using or accessing ProMobi products, you indicate your assent to be bound by this Agreement.

Scope of the Agreement: This Agreement governs your initial purchase as well as any future purchases made by you that reference this Agreement. This Agreement includes our [Privacy Policy](#), our [Acceptable Use Policy](#), any Orders, and any other referenced policies and attachments. This Agreement applies to Scalefusion add-ons or plugins that you purchase from the Scalefusion website or from authorised resellers and distributors. However, it does not apply to apps, add-ons or plugins from other vendors that you install on your managed devices.

The “**Effective Date**” of this Agreement is the date which is the earlier of (a) Customer’s initial access to any Service (as defined below) through any online provisioning, registration or order process or (b) the effective date of the first Order Form referencing this Agreement.

As used in this Agreement, “ProMobi” means (a) ProMobi Technologies Pvt. Ltd., an Indian corporation with registered office at 303, Welworth Classic PLNo:2+3, SNo: 22/2, Wadgaonsheri, Pune, MH 411014, India.

ProMobi Products: This agreement governs (A) ProMobi’s software subscriptions to online software-as-a-service products

Account Registration

Revisions to this agreement: From time to time, ProMobi may modify this Agreement. Unless otherwise specified by ProMobi, changes to this term will be effective upon renewal of Customer’s current Subscription Term (as defined below) or entry into a new purchase order form. ProMobi will use reasonable effort to inform Customer of the changes through communications via Customer’s account, email or other means. In some cases Customer may be required to click to accept the new

terms or otherwise agree to the modified agreement before renewing the Subscription Term or entering into a new purchase order form, and in any event continued use of the ProMobi's products or services after the updated terms of this Agreement goes into effect will constitute Customer's acceptance of such updated terms. If ProMobi specifies that changes to the new terms will take effect prior to Customer's next renewal or purchase order (due to legal compliance or product change reasons) and Customer objects to such changes, Customer may terminate the applicable Subscription Term and receive as its sole remedy a refund of any fees Customer has pre-paid for use of the applicable Services for the terminated portion of the Subscription Term.

BY INDICATING YOUR ACCEPTANCE OF THIS AGREEMENT OR ACCESSING OR USING ANY SERVICES, YOU ARE AGREEING TO BE BOUND BY ALL TERMS, CONDITIONS, AND NOTICES CONTAINED OR REFERENCED IN THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, PLEASE DO NOT USE ANY SERVICES. FOR CLARITY, EACH PARTY EXPRESSLY AGREES THAT THIS AGREEMENT IS LEGALLY BINDING UPON IT. THIS AGREEMENT CONTAINS MANDATORY ARBITRATION PROVISIONS THAT REQUIRE THE USE OF ARBITRATION TO RESOLVE DISPUTES, RATHER THAN JURY TRIALS. PLEASE READ IT CAREFULLY.

1. Definitions

“Scalefusion (formerly MobiLock)” or “Scalefusion (formerly MobiLock Pro)” means a proprietary Enterprise Mobility Management solution developed, owned and marketed by ProMobi as software-as-a-service solution. In this agreement it will further be referred as **“Scalefusion”** only.

“Affiliate” means any entity under the control of Customer where “control” means ownership of or the right to control greater than 50% of the voting securities of such entity.

“AUP” means ProMobi's [Acceptable Use Policy](#).

“Contractor” means an independent contractor or consultant who is not a competitor of ProMobi.

“Customer Data” means any data of any type that is submitted to the Services by or on behalf of Customer, including without limitation: (a) data submitted, uploaded or imported to the Services by Customer (including from Third Party Platforms) and (b) data provided by or about People (including chat and message logs) that are collected from the Customer use of the Services.

“Customer Properties” means Customer's devices, apps, files owned and operated by (or for the benefit of) Customer through which Customer uses the Services to manage their account and devices.

“Dashboard” means Scalefusion's user interface for accessing and administering the Services that Customer may access via the web or the Scalefusion Apps.

“Documentation” means the technical user documentation provided with the Services.

“Feedback” means comments, questions, suggestions or other feedback relating to

any ProMobi product or service.

“ProMobi App” means any mobile application or desktop client software included in the applicable Service that is made available by ProMobi.

“Laws” means all applicable local, state, federal and international laws, regulations and conventions, including, without limitation, those related to data privacy and data transfer, international communications, and the exportation of technical or personal data.

“People” (in the singular, “Person”) means Customer’s end user customers, potential customers, and other users of and visitors to the Customer Properties.

“Permitted User” means an employee or Contractor of Customer or its Affiliate who is authorized to access the Service.

“Sensitive Personal Information” means any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards (“PCI DSS”); (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (“HIPAA”); or (iii) any other personal data of an EU citizen deemed to be in a “special category” (as identified in EU Data Protection Directive 95/46/EC or any successor directive or regulation).

“Services” means ProMobi’s proprietary software-as-a-service solution(s), including the Dashboard, Scalefusion application programming interfaces (APIs), Scalefusion Code and Scalefusion Add-on Apps, Scalefusion JavaScript APIs, Scalefusion Developer APIs as described in the applicable purchase order form.

“Taxes” means any sales, use, GST, value-added, withholding, or similar taxes or levies, whether domestic or foreign, other than taxes based on the income of ProMobi.

“Third-Party Platform” means any software, software-as-a-service, data sources or other products or services not provided by ProMobi that are integrated with Services as described in the Documentation.

2. ProMobi Services

2.1. Services Overview: ProMobi’s Services are a suite of mobility software-as-a-service solutions offered through a single platform. The Services are designed to enable Customer to manage their corporate owned devices and to provide a Dashboard for accessing and managing Customer Data regarding those devices. Customer may import and export Customer Data between the Services and certain Third-Party Platforms through supported integrations. The Services also include ProMobi Apps or Code deployed on Customer Properties (i.e devices) to enable management functionality.

2.2. Provision of Services: Each Service is provided on a subscription basis for a set term designated on the purchase order form (each, a “Subscription Plan”). ProMobi may also offer Professional Services (as defined in Section 11) related to certain Services. Customer will purchase and ProMobi will provide the specific Services and related Professional Services (if any) as specified in the applicable purchase order form.

2.3. Access to Services: Customer may access and use the Services solely for its own benefit and in accordance with the terms and conditions of this Agreement, the Documentation and any scope of use restrictions designated in the applicable purchase order form (including without limitation the number of devices managed). Use of and access to the Services is permitted only by Permitted Users. If Customer is given API keys or passwords to access the Services on ProMobi's systems, Customer will require that all Permitted Users keep API keys, user ID and password information strictly confidential and not share such information with any unauthorized person. User IDs are granted to individual, named persons and may not be shared. If Customer is accessing the Services using credentials provided by a third party (e.g., Google), then Customer will comply with all applicable terms and conditions of such third party regarding provisioning and use of such credentials. Customer will be responsible for any and all actions taken using Customer's accounts and passwords. If any Permitted User who has access to a user ID is no longer an employee (or Contractor, as set forth below) of Customer, then Customer will immediately delete such user ID and otherwise terminate such Permitted User's access to the Service. The right to use the Services includes the right to deploy ProMobi Apps and Code on Customer Properties in order to enable device management, monitoring and similar functionality and to collect Customer Data for use with the Services as further described below.

2.4. ProMobi Apps: To the extent ProMobi provides ProMobi Apps for use with the Services, subject to all of the terms and conditions of this Agreement, ProMobi grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to use the object code form of the ProMobi Apps internally, but only in connection with Customer's use of the Service and otherwise in accordance with the Documentation and this Agreement.

2.5. Deployment of ProMobi Apps: Subject to all of the terms and conditions of this Agreement, ProMobi grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during any applicable Subscription Term to deploy the ProMobi Apps in the form provided by ProMobi on Customer Properties solely to support Customer's use of the Service and otherwise in accordance with the Documentation and this Agreement. Customer must install ProMobi Apps on the Customer Properties in order to enable features of the Services. Customer will deploy all ProMobi Apps in strict accordance with the Documentation and other instructions provided by ProMobi. Customer acknowledges that any changes made to the Customer Properties after initial deployment of ProMobi Code may cause the Services to cease working or function improperly and that ProMobi will have no responsibility for the impact of any such Customer changes.

2.6. Contractors and Affiliates: Customer may permit its Contractors and its Affiliates' employees and Contractors to serve as Permitted Users, provided Customer remains responsible for compliance by such individuals with all of the terms and conditions of this Agreement, and any use of the Services by such individuals is for the sole benefit of Customer.

2.7. General Restrictions: Customer will not (and will not permit any third party to): (a) rent, lease, provide access to or sublicense the Services to a third party; (b) use the Services to provide, or incorporate the Services into, any product or service provided to a third party; © reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to the Services, except to the extent expressly permitted by applicable law (and then only upon advance notice to ProMobi); (d) copy or modify the Services or any Documentation, or create any

derivative work from any of the foregoing; (e) remove or obscure any proprietary or other notices contained in the Services (including without limitation (i) the “Powered by Scalefusion” designation that may appear as part of the deployment of the Services on Customer Properties and (ii) notices on any reports or data printed from the Services); or (f) publicly disseminate information regarding the performance of the Services.

2.8. Scalefusion APIs: If ProMobi makes access to any APIs available as part of the Services, then ProMobi reserves the right to place limits on access to such APIs (e.g., limits on numbers of calls or requests). Further, ProMobi may monitor Customer’s usage of such APIs and limit the number of calls or requests Customer may make if ProMobi believes that Customer’s usage is in breach of this Agreement or may negatively affect the Services (or otherwise impose liability on ProMobi).

2.9. Trial Subscriptions: If Customer receives free access or a trial or evaluation subscription to the Service (a “Trial Subscription”), then Customer may use the Services in accordance with the terms and conditions of this Agreement for a period of fourteen (14) days or such other period granted by ProMobi (the “Trial Period”). Trial Subscriptions are permitted solely for Customer’s use to determine whether to purchase a paid subscription to the Services. Trial Subscriptions may not include all functionality and features accessible as part of a paid Subscription Term. If Customer does not enter into a paid Subscription Term, this Agreement and Customer’s right to access and use the Services will terminate at the end of the Trial Period. ProMobi has the right to terminate a Trial Subscription at any time for any reason.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ProMobi WILL HAVE NO WARRANTY, INDEMNITY, SUPPORT, OR OTHER OBLIGATIONS WITH RESPECT TO TRIAL SUBSCRIPTIONS.

3. Customer Data

3.1. Rights in Customer Data: As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data as provided to ProMobi. Subject to the terms of this Agreement, Customer hereby grants to ProMobi a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data solely to the extent necessary to provide the Services to Customer.

3.2. Storage of Customer Data: ProMobi does not provide any long term archiving service. ProMobi agrees only that it will not intentionally delete any Customer Data from any Service prior to termination of Customer’s applicable Subscription Term. ProMobi expressly disclaims all other obligations with respect to storage.

3.3. Customer Obligations

a) *In General* Customer is solely responsible for the accuracy, content and legality of all Customer Data. Customer represents and warrants to ProMobi that Customer has all necessary rights, consents and permissions to collect, share and use all Customer Data as contemplated in this Agreement (including granting ProMobi the rights in Section 3.1 (Rights in Customer Data)) and that no Customer Data will violate or infringe (i) any third party intellectual property, publicity, privacy or other rights, (ii) any Laws, or (iii) any terms of service, privacy policies or other agreements governing the Customer Properties or Customer’s accounts with any Third-Party Platforms. Customer further represents and warrants that all Customer Data complies with the

AUP. Customer will be fully responsible for any Customer Data submitted to the Services by any Person as if it was submitted by Customer.

b) *No Sensitive Personal Information.* Customer specifically agrees not to use the Services to collect, store, process or transmit any Sensitive Personal Information. Customer acknowledges that ProMobi is not a Business Associate or subcontractor (as those terms are defined in HIPAA) or a payment card processor and that the Services are neither HIPAA nor PCI DSS compliant. ProMobi will have no liability under this Agreement for Sensitive Personal Information, notwithstanding anything to the contrary herein.

c) *Compliance with Laws.* Customer agrees to comply with all applicable Laws in its use of the Services. Without limiting the generality of the foregoing, Customer will not engage in any unsolicited advertising, marketing, or other activities using the Services, including without limitation any activities that violate the Telephone Consumer Protection Act of 1991, CAN-SPAM Act of 2003 or any other anti-spam laws and regulations.

3.4. Indemnification by Customer: Customer will indemnify, defend and hold harmless ProMobi from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with any claim arising from or relating to any Customer Data or breach or alleged breach by Customer of Section 3.3 (Customer Obligations). This indemnification obligation is subject to Customer receiving (i) prompt written notice of such claim (but in any event notice in sufficient time for Customer to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense, or settlement of such claim; and (iii) all necessary cooperation of ProMobi at Customer's expense. Notwithstanding the foregoing sentence, (a) ProMobi may participate in the defense of any claim by counsel of its own choosing, at its cost and expense and (b) Customer will not settle any claim without ProMobi's prior written consent, unless the settlement fully and unconditionally releases ProMobi and does not require ProMobi to pay any amount, take any action, or admit any liability.

3.5. Aggregated Anonymous Data: Notwithstanding anything to the contrary herein, Customer agrees that ProMobi may obtain and aggregate technical and other data about Customer's use of the Services that is non-personally identifiable with respect to Customer ("Aggregated Anonymous Data"), and ProMobi may use the Aggregated Anonymous Data to analyze, improve, support and operate the Services and otherwise for any business purpose during and after the term of this Agreement, including without limitation to generate industry benchmark or best practice guidance, recommendations or similar reports for distribution to and consumption by Customer and other ProMobi customers. For clarity, this Section 3.5 does not give ProMobi the right to identify Customer as the source of any Aggregated Anonymous Data.

4. Security

ProMobi agrees to use commercially reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of any Service or Customer Data. However, ProMobi will have no responsibility for errors in transmission, unauthorized third-party access or other causes beyond ProMobi's control. Visit ProMobi's [security practices](#) here.

5. Third-Party Platform Integrations

The Services may support integrations with certain Third-Party Platforms. In order for the Services to communicate with such Third-Party Platforms, Customer may be required to input credentials in order for the Services to access and receive relevant information from such Third-Party Platforms. By enabling use of the Services with any Third-Party Platform, Customer authorizes ProMobi to access Customer's accounts with such Third-Party Platform for the purposes described in this Agreement. Customer is solely responsible for complying with any relevant terms and conditions of the Third-Party Platforms and maintaining appropriate accounts in good standing with the providers of the Third-Party Platforms. Customer acknowledges and agrees that ProMobi has no responsibility or liability for any Third-Party Platform or any Customer Data exported to a Third-Party Platform. ProMobi does not guarantee that the Services will maintain integrations with any Third-Party Platform and ProMobi may disable integrations of the Services with any Third-Party Platform at any time with or without notice to Customer. For clarity, this Agreement governs Customer's use of and access to the Services, even if accessed through an integration with a Third-Party Platform.

6. Ownership

6.1. **Scalefusion Technology_**: This is a subscription agreement for access to and use of the Services. Customer acknowledges that it is obtaining only a limited right to the Services and that irrespective of any use of the words "purchase", "sale" or like terms in this Agreement no ownership rights are being conveyed to Customer under this Agreement. Customer agrees that ProMobi or its suppliers retain all right, title and interest (including all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the Services and all Documentation, professional services deliverables and any and all related and underlying technology and documentation and any derivative works, modifications or improvements of any of the foregoing, including as may incorporate Feedback (collectively, "**Scalefusion Technology**"). Except as expressly set forth in this Agreement, no rights in any **Scalefusion Technology** are granted to Customer. Further, Customer acknowledges that the Services are offered as an on-line, hosted solution, and that Customer has no right to obtain a copy of any of the Services, except for ProMobi Code and the ProMobi Apps in the format provided by ProMobi.

6.2. **Feedback**. Customer, from time to time, may submit Feedback to ProMobi. ProMobi may freely use or exploit Feedback in connection with any of its products or services.

7. Subscription Term, Fees & Payment

7.1. **Subscription Term and Renewals**: Unless otherwise specified on the applicable purchase order, each Subscription Term will have to be renewed explicitly, you will receive an email notification about the expiry of your Subscription Term at least thirty (30) days prior to expiration of the then-current Subscription Term.

7.2. **Fees and Payment**: All fees are as set forth in the applicable purchase order and will be paid by Customer within thirty (30) days of invoice, unless (a) Customer is paying via Credit Card (as defined below) or (b) otherwise specified in the applicable purchase order. Except as expressly set forth in Section 9 (Limited Warranty) and Section 14 (Indemnification), all fees are non-refundable. The rates in the purchase

order and/or invoices are valid for the initial twelve (12) month period of each Subscription Term and thereafter may be subject to an automatic adjustment increase of up to ten percent (10%) per year. Customer is responsible for paying all Taxes, and all Taxes are excluded from any fees set forth in the applicable purchase order. If Customer is required by Law to withhold any Taxes from Customer's payment, the fees payable by Customer will be increased as necessary so that after making any required withholdings, ProMobi receives and retains (free from any liability for payment of Taxes) an amount equal to the amount it would have received had no such withholdings been made. Any late payments will be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less.

7.3. Payment Via Credit Card: If you are purchasing the Services via credit card, debit card or other payment card ("Credit Card"), the following terms apply:

- **Foreign Transaction Fees.** Customer acknowledges that for certain Credit Cards, the issuer of Customer's Credit Card may charge a foreign transaction fee or other charges.
- **Invalid Payment:** If a payment is not successfully settled due to expiration of a Credit Card, insufficient funds, or otherwise, Customer remains responsible for any amounts not remitted to ProMobi and ProMobi may, in its sole discretion, either (i) invoice Customer directly for the deficient amount, or (ii) terminate the Subscription Term as well as this Agreement.
- **Payment of Outstanding Fees.** Upon any termination or expiration of the Subscription Term, ProMobi will invoice Customer directly for any outstanding fees for Customer's use of the Services during the Subscription Term, after which ProMobi will not charge for any additional fees, once the outstanding amount is paid in full.

7.4. Suspension of Service. If Customer's account is thirty (30) days or more overdue, in addition to any of its other rights or remedies (including but not limited to any termination rights set forth herein), ProMobi reserves the right to suspend Customer's access to the applicable Service (and any related services) without liability to Customer until such amounts are paid in full. ProMobi also reserves the right to suspend Customer's access to the Services without liability to Customer if Customer's use of the Services is in violation of the AUP.

7.5. Subscription Downgrade. Customer cannot downgrade their plan in the middle of an existing active subscription. However, customers can downgrade their plan at the renewal of their existing subscription. The newly chosen plan will be effective only after the renewal. Customers can choose to downgrade to the then-available subscription plan while renewal.

7.6. Subscription Plan. ProMobi reserves the right to change its offering of subscription plans, including by limiting or ceasing to offer any subscription plans, including any associated features as well, upon sending a written notice to Customer, which may be by email. Subscription plans may not be available to all customers and regions.

8. Term and Termination

8.1. Term. This Agreement is effective as of the Effective Date and expires on the date of expiration or termination of all Subscription Terms.

8.2. Termination for Cause. Either party may terminate this Agreement (including all related purchase orders) if the other party (a) fails to cure any material breach of this Agreement (including a failure to pay fees) within thirty (30) days after written notice; (b) ceases operation without a successor; or © seeks protection under any bankruptcy, receivership, trust deed, creditors' arrangement, composition, or comparable proceeding, or if any such proceeding is instituted against that party (and not dismissed within sixty (60) days thereafter).

8.3. Effect of Termination. Upon any expiration or termination of this Agreement, Customer will immediately cease any and all use of and access to all Services (including any and all related Scalefusion Technology) and delete (or, at ProMobi's request, return) any and all copies of the Documentation, any Scalefusion passwords or access codes and any other ProMobi Confidential Information in its possession. Provided this Agreement was not terminated for Customer's breach, Customer may retain and use internally copies of all reports exported from any Service prior to termination. Customer acknowledges that following termination it will have no further access to any Customer Data input into any Service, and that ProMobi may delete any such data as may have been stored by ProMobi at any time. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law or otherwise.

8.4. Survival. The following Sections will survive any expiration or termination of this Agreement: 2.7 (General Restrictions), 2.9 (Trial Subscriptions), 3.2 (Storage of Customer Data), 3.4 (Indemnification by Customer), 3.5 (Aggregated Anonymous Data), 6 (Ownership), 7.2 (Fees and Payment), 7.3 (Payment Via Credit Card), 8 (Term and Termination), 9.2 (Warranty Disclaimer), 12 (Limitation of Remedies and Damages), 13 (Indemnification), 14 (Confidential Information) and 16 (General Terms).

9. Limited Warranty

9.1. Limited Warranty: ProMobi warrants, for Customer's benefit only, that each Service will operate in substantial conformity with the applicable Documentation. ProMobi's sole liability (and Customer's sole and exclusive remedy) for any breach of this warranty will be, at no charge to Customer, for ProMobi to use commercially reasonable efforts to correct the reported non-conformity, or if ProMobi determines such remedy to be impracticable, either party may terminate the applicable Subscription Term and Customer will receive as its sole remedy a refund of any fees Customer has pre-paid for use of such Service for the terminated portion of the applicable Subscription Term. The limited warranty set forth in this Section 9.1 will not apply: (i) unless Customer makes a claim within thirty (30) days of the date on which Customer first noticed the non-conformity, (ii) if the error was caused by misuse, unauthorized modifications or third-party hardware, software or services, or (iii) to use provided on a no-charge, trial or evaluation basis.

9.2. Warranty Disclaimer: EXCEPT FOR THE LIMITED WARRANTY IN SECTION 9.1, ALL Services and PROFESSIONAL SERVICES ARE PROVIDED "AS IS". NEITHER PROMOBI NOR ITS SUPPLIERS MAKES ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. ProMobi does not warrant that Customer's use of THE Services will be uninterrupted or error-free, nor does ProMobi

warrant that it will review the Customer Data for accuracy or that it will preserve or maintain the Customer Data without loss OR CORRUPTION. PROMOBI SHALL NOT BE LIABLE FOR THE RESULTS OF ANY COMMUNICATIONS SENT OR ANY COMMUNICATIONS THAT WERE FAILED TO BE SENT USING THE SERVICES. ProMobi SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES OR OTHER PROBLEMS INHERENT IN USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS, THIRD-PARTY PLATFORMS OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF ProMobi. CUSTOMER MAY HAVE OTHER STATUTORY RIGHTS, BUT THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE SHORTEST PERIOD PERMITTED BY LAW.

10. Support

During the Subscription Term of each Service, ProMobi will provide end user support in accordance with ProMobi's [Support Policy](#) ("Support Policy").

11. Professional Services

ProMobi may provide the professional consulting services ("Professional Services") purchased in the applicable purchase order. The scope of Professional Services will be as set forth in a Statement of Work ("SOW") referencing this Agreement and executed by both parties describing the work to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information ("SOW"). Unless Professional Services are provided on a fixed-fee basis, Customer will pay ProMobi at the per-hour rates set forth in the Purchase Order Form (or, if not specified, at ProMobi's then-standard rates) for any excess services. Customer will reimburse ProMobi for reasonable travel and lodging expenses as incurred. Customer may use anything delivered as part of the Professional Services in support of authorized use of the Services and subject to the terms regarding Customer's rights to use the Service set forth in Section 2 (ProMobi Services) and the applicable SOW, but ProMobi will retain all right, title and interest in and to any such work product, code or deliverables and any derivative, enhancement or modification thereof created by ProMobi (or its agents).

12. Limitation of Remedies and Damages

12.1. Consequential Damages Waiver. EXCEPT FOR EXCLUDED CLAIMS (DEFINED BELOW), NEITHER PARTY (NOR ITS SUPPLIERS) SHALL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOSS OF USE, LOST DATA, LOST PROFITS, FAILURE OF SECURITY MECHANISMS, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12.2. Liability Cap. PROMOBI'S AND ITS SUPPLIERS' ENTIRE LIABILITY TO CUSTOMER ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY CUSTOMER TO PROMOBI DURING THE PRIOR TWELVE (12) MONTHS UNDER THIS AGREEMENT.

12.3. Excluded Claims. "Excluded Claims" means any claim arising (a) from Customer's breach of Section 2.7 (General Restrictions); (b) under Section 3.3 (Customer Obligations) or 3.4 (Indemnification by Customer); or © from a party's

breach of its obligations in Section 15 (Confidential Information) (but excluding claims arising from operation or non-operation of any Service).

12.4. Nature of Claims and Failure of Essential Purpose. The parties agree that the waivers and limitations specified in this Section 13 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy specified in this Agreement is found to have failed of its essential purpose.

13. Indemnification

ProMobi will defend Customer from and against any claim by a third party alleging that a Service when used as authorized under this Agreement infringes a U.S. patent, U.S. copyright, or U.S. trademark and will indemnify and hold harmless Customer from and against any damages and costs finally awarded against Customer or agreed in settlement by ProMobi (including reasonable attorneys' fees) resulting from such claim, provided that ProMobi will have received from Customer: (i) prompt written notice of such claim (but in any event notice in sufficient time for ProMobi to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense and settlement (if applicable) of such claim; and (iii) all reasonable necessary cooperation of Customer. If Customer's use of a Service is (or in ProMobi's opinion is likely to be) enjoined, if required by settlement or if ProMobi determines such actions are reasonably necessary to avoid material liability, ProMobi may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for Customer the right to continue using such Service; or if (a) and (b) are not commercially reasonable, © terminate this Agreement and refund to Customer the fees paid by Customer for the portion of the Subscription Term that was paid by Customer but not rendered by ProMobi. The foregoing indemnification obligation of ProMobi will not apply: (1) if such Service is modified by any party other than ProMobi, but solely to the extent the alleged infringement is caused by such modification; (2) if such Service is combined with products or processes not provided by ProMobi, but solely to the extent the alleged infringement is caused by such combination; (3) to any unauthorized use of such Service; (4) to any action arising as a result of Customer Data or any third-party deliverables or components contained within such Service; (5) to the extent the alleged infringement is not caused by the particular technology or implementation of the Service but instead by features common to any similar product or service; or (6) if Customer settles or makes any admissions with respect to a claim without ProMobi's prior written consent. THIS SECTION 13 SETS FORTH ProMobi's AND ITS SUPPLIERS' SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

14. Confidential Information

Each party (as "**Receiving Party**") agrees that all code, inventions, know-how, business, technical and financial information it obtains from the disclosing party ("**Disclosing Party**") constitute the confidential property of the Disclosing Party ("**Confidential Information**"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be confidential or proprietary due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any Scalefusion Technology, performance information relating to any Service, and the terms and conditions of this Agreement will be deemed Confidential Information of ProMobi without any marking or further

designation. Except as expressly authorized herein, the Receiving Party will (1) hold in confidence and not disclose any Confidential Information to third parties and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement. The Receiving Party may disclose Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know (including, for ProMobi, the subcontractors referenced in Section 17.8 (Subcontractors)), provided that such representatives are bound to confidentiality obligations no less protective of the Disclosing Party than this Section 14 and that the Receiving Party remains responsible for compliance by any such representative with the terms of this Section 14. The Receiving Party's confidentiality obligations will not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information. The Receiving Party may make disclosures to the extent required by law or court order, provided the Receiving Party notifies the Disclosing Party in advance and cooperates in any effort to obtain confidential treatment. The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

15. Co-Marketing

At the request of ProMobi, Customer may agree to participate in other reasonable marketing activities that promote the benefits of the Services to other potential customers and to use of Customer's name and logo on ProMobi's web site and in ProMobi promotional materials. Customer agrees that ProMobi may disclose Customer as a customer of ProMobi.

16. General Terms

16.1. Assignment: This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in connection with a merger, reorganization, acquisition or other transfer of all or substantially all of such party's assets or voting securities. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section 16.1 will be null and void.

16.2. Severability: If any provision of this Agreement will be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect.

16.3. Entire Agreement: This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement. Customer acknowledges that the Services are on-line, subscription-based products, and that in order to provide improved customer experience ProMobi

may make changes to the Services, and ProMobi will update the applicable Documentation accordingly. The support terms described in the Support Policy may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices (but the modifications will not materially decrease ProMobi's obligations as compared to those reflected in such terms as of the Effective Date).

16.4. Force Majeure: Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events that occur after the signing of this Agreement and that are beyond the reasonable control of such party, such as a strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or telecommunications or data networks or services, or refusal of a license by a government agency.

16.5. Subcontractors: ProMobi may use the services of subcontractors and permit them to exercise the rights granted to ProMobi in order to provide the Services under this Agreement, provided that ProMobi remains responsible for (i) compliance of any such subcontractor with the terms of this Agreement and (ii) for the overall performance of the Services as required under this Agreement.

16.6. Subpoenas: Nothing in this Agreement prevents ProMobi from disclosing Customer Data to the extent required by law, subpoenas, or court orders, but ProMobi will use commercially reasonable efforts to notify Customer where permitted to do so.

16.7 Changes to this Agreement. We may update or modify this Agreement from time to time, including any referenced policies and other documents. If a revision meaningfully reduces your rights, we will use reasonable efforts to notify you (by, for example, sending an email to the billing or technical contact you designate in the applicable purchase Order, posting on our blog, through your ProMobi account, or in the Product itself). If we modify the Agreement during your License Term or Subscription Term, the modified version will be effective upon your next renewal of a License Term, Support and Maintenance term, or Subscription Term, as applicable. In this case, if you object to the updated Agreement, as your exclusive remedy, you may choose not to renew, including cancelling any terms set to auto-renew. With respect to No-Charge Products, accepting the updated Agreement is required for you to continue using the No-Charge Products. You may be required to click through the updated Agreement to show your acceptance. If you do not agree to the updated Agreement after it becomes effective, you will no longer have a right to use No-Charge Products. For the avoidance of doubt, any purchase Order is subject to the version of the Agreement in effect at the time of the Order.

16.8. Counterparts: This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

ACCELERATING BUSINESS WITH SPOORS – EFFORT FIELD SERVICE MANAGEMENT IN THE CLOUD

If your business need advance functionalities for managing Service orders, Dispatching technicians, Work planning, Route optimization Effort is the product. Built for the cloud, Effort Field Service Management has enabled staff to work on the go, helping the highest performing service organizations tackle a new generation of field service challenges.

Cloud solutions to field service management means there's no infrastructure to manage, making it easy to provision new operations, upscale or add more functionalities as soon as you need it.

Cloud-based solutions are very attractive for field service because they may be more flexible, readily extensible and more accessible being cost effective.



High on Configurability

The advantages of using effort is the enhanced operational flexibility and agility it gives your business. Our cloud services support options for configuration, customization & integrations and it provides the choice of when to deploy updates, except for mandatory essential patches.

Unique Value proposition

1. Dynamic Mobile **Form engine**
2. **Offline Mobile App** for IOS & Android Devices
3. Flexibility to Capture Images, Videos, Audio
4. **Geotagging** of Activities



GENERAL TERMS AND CONDITION

- Signup/registration on the Website/App is available only to the person who can form legally binding contracts under Indian Contract Act, 1872. Persons who are "incompetent to contract" within the meaning of the Indian Contract Act, 1872 including minors, un-discharged insolvents etc. are not eligible to register on the Website/App. As a minor if User wish to use the Website/App, shall be registered by legal guardian or parents on the Website/App. If it comes to the knowledge of Spoors Private Limited that the User registered on the Website/App via providing the personal information is under the age of 18 years, shall be removed from the Website/App by Spoors Private Limited. Spoors Private Limited reserves the right to terminate the membership and / or refuse to provide the User with access to the Website/App if it is brought to Spoors Private Limited notice or if it is discovered that the signup/registration over the Website/App is done by a User, under the age of 18 years.
- Signup/registration of the User on the Website/App is necessary to access the Website/App and use the services. User shall be required to signup/register for an account on the Website/App by providing email address, name, password and user name. User shall provide accurate, complete and updated information in order to signup/register on the Website/App to use the services.
- User represent, warrant, and agree that User shall not use the services in a manner that:
 1. Infringes or violates the intellectual property rights or any other rights of anyone else.
 2. Violates any law or regulation;
 3. Is harmful, fraudulent, deceptive, threatening, harassing, defamatory, obscene, or otherwise objectionable;

4. Attempts, in any manner, to obtain the password, account, or other security information from any other User;
 5. Violates the security of any computer network, or cracks any passwords, or security encryption codes;
- User accepts the Website/App Terms and condition, Privacy Policy by using the “OTP” to signup/register when registering and logging into the Website/App to use the services.
 - Spoors Private Limited might change the methodology or functionality of the Website/App at any point of time and intimation to that extent shall be mentioned in the Website/App under Terms and Conditions.
 - Spoors Private Limited shall always try to improve the services provided by the Website/App which shall include suspension or discontinuation of any part of the services. Spoors Private Limited shall introduce features or impose limit on certain features or restrict access to parts or all of the services provided through the Website/App. A notification of any such action shall be sent to the User in advance.
 - Spoors Private Limited reserves the right to remove any content provided on the Website/App at any time without any reason or any notice of any such action by Spoors Private Limited on the Website/App. Subject to the terms and conditions set forth in this Agreement. Spoors Private Limited grants User a non-exclusive, non-transferable, limited right to access and use this Website/App and the information thereon. User agrees not to interrupt or attempt to interrupt the services of the Website/App in any way.
 - The information provided on the Website/App are in relation to providing services such as text, graphics, article, photos, images are protected by the Copyright and other Intellectual Property Laws. User promises to abide by all Copyright notices, Trademark rules and the User won't use, copy, reproduce, modify, translate, publish, broadcast, transmit, distribute, perform, upload, display, license, sell or otherwise exploit for any purpose any Content not owned by the User without the prior written consent of Spoors Private Limited. User won't modify, publish, transmit, participate in the transfer or sale

of, reproduce, create derivative works based on, or otherwise exploit any of the Services.

- The information on this Website/App has been included in good faith and is for general purposes only. It should not be relied upon for any specific purpose and no representation or warranty is given as regards its accuracy or completeness.
- No reproduction of any part of the Website/App may be sold or distributed for commercial gain, nor shall it be modified or incorporated in any other work, publication or site, whether in hard copy or electronic format, including postings to any other site. Spoors Private Limited reserves all other rights.
- Neither Spoors Sons and Spoors affiliates, nor their affiliates' officers, employees or agents shall be liable for any loss, damage or expense arising out of any access to or use of this Website/App including without limitation, any loss of profit, indirect, incidental or consequential loss.
- In relation to any circumstances that arise due to the Use of the Website/App shall be communicated to the customer care of the Website/App. User understands that there may be instances of difficulty in accessing or receiving email communication. We are not responsible if any email notice gets caught by User's SPAM folder, or if User do not see the email, or if User has given us an incorrect email id or if for any other reason You do not receive the email notice. Therefore, we encourage User to frequently open the Application to monitor any changes. User continued use of or access to the Services following the posting of any changes to this Agreement constitutes acceptance of those changes.
- Any failure of functioning of the Website/App shall be intimated by the User to Spoors Private Limited and Spoors Private Limited shall duly try to resolve the issue. Spoors Private Limited shall not be liable for any kind of damages or losses faced by the User due to functionality of the Website/App.

- Payment of such services shall be in accordance to the charges available on the app store during purchase of such services, or as informed by Spoors Private Limited to the User based on the services availed.
- Spoors Private Limited will protect the data to the extent required by applicable law, and subject to applicable law, Spoors Private Limited will take every security measure for protection of the data provided. Spoors Private Limited will not disclose any information to any third-party and will not engage directly with another processor to provide the Services to the User. Spoors Private Limited will keep records of its processing activities with respect to any data and cooperate with authorized person in respect of any complaint or investigation relating to such data. Website/App will notify the User in respect of any suspected or actual breach of data security or other unauthorized access or processing of any such data .
- User agrees to indemnify and hold Spoors Private Limited, its affiliates, officers, agents, employees, and partners harmless for and against any and all claims, liabilities, damages (actual and consequential), losses and expenses (including attorneys' fees) arising from or in any way related to any third party claims relating to (a) User's use of the Services (including any actions taken by a third party using User account), and (b) User's violation of these Terms. In the event of such a claim, suit, or action, Spoors Private Limited shall provide notice of the claim to the contact information provided by the User during signup/registration on the Website/App. Failure to deliver such notice shall not eliminate or reduce User's indemnification obligations hereunder.
- Spoors Private Limited shall own all rights, title, and interest in the feedback provided by the User and Spoors Private Limited shall be entitled to use the feedback without restriction, even if the User has indicated such feedback as confidential or restricted for improvement of Website/App services. Website/App shall not be under any obligation of confidentiality, express or implied, with respect to the feedback. Spoors Private Limited shall be entitled to use or disclose any such feedback for any purpose, in any

way required and Spoors Private Limited will not be liable for any compensation for any such disclosure under any circumstances.

- Spoors Private Limited will suspend the Users right to use the services immediately upon notice of any security risk due to the Users use of the services which may impact the App or other systems or if it comes to the knowledge of any fraudulent use of Website/App.
- This Agreement is the complete and exclusive statement of the agreements between User and Spoors Private Limited with respect to the subject matter hereof and supersedes all other communications or representations or agreements (whether oral, written or otherwise) relating thereto.
- The failure of either party at any time to require performance of any provision of this Agreement in no manner shall affect such party's right at a later time to enforce the same. No waiver by either party of any breach of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be, or construed as, a further or continuing waiver of any other such breach, or a waiver of any other breach of this Agreement.
- If any provision of this Agreement shall to any extent be held invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions of this Agreement shall in no way be affected or impaired thereby and each such provision of this Agreement shall be valid and enforceable to the fullest extent permitted by law. In such case, this Agreement shall be reformed to the minimum extent necessary to correct any invalidity, illegality or unenforceability, while preserving to the maximum extent the rights and commercial expectations of the parties hereto, as expressed herein.
- These Terms are governed by and will be construed under the laws of India, without regard to the conflicts of laws provisions thereof, unless prohibited by law. Any dispute arising from or relating to the subject matter of these Terms shall be finally settled in

Hyderabad, India. THIS CLAUSE SHALL SURVIVE THE TERMINATION OR EXPIRY OF THIS AGREEMENT.

- **I AGREE TO THE ABOVE TERMS AND CONDITIONS**

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory F: Mobile Data Collection/Mobile Forms

Subcategory I: Public Safety Systems

Subcategory M: Enterprise Messaging

Client Company name:

Tennessee Trash Service Solution

Client name of contact:

Steve Turner

Client contact title:

Owner

Client is a daily user, occasional user, etc.:

Daily

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Kevin Dylla no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

Vendor used: Team On The Run by StreamWIDE

Steve Turner, Owner

Cell: 865-740-7771

stevet@tntrashservice.com

Licenses: 68 Team on The Run licenses

Tennessee Trash Service is a residential & commercial garbage removal company located in Knoxville, Tennessee. We were interested in a new fleet solution for drivers covering a 100-mile radius of Knoxville with different routes every day. We were using push to talk on basic phones to dispatch the entire fleet, which was inefficient, noisy and chaotic by giving verbal turn by turn directions and also trying to determine drivers' locations to pick up misses. Fleet solution would need to refresh data more frequently to have more accurate speed alerts to enforce safety policies. Lastly, we wanted to see all of the routes in the fleet management portal to ensure route optimization.

2. Would you recommend USCC to other customers? Why?

Yes, because the product is easy to use, saves time and saves money.

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

Met milestones

4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?

5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?

Replacing basic driver phones with ruggedized smart phones with Team on the Run for push to talk capability helped making the dispatch process easier & more productive by pushing out Google Map links to drivers for direction, drivers sending pictures/videos from the field, group messaging reducing the chatter in dispatch. MaaS360 locked down the driver smartphones only allowing access to phone calls, Team on the Run, Weather and Google Maps.

6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?

N/A

7. Is there anything else you think we should know about working with USCC or using USCC's products and services?

N/A

8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?

None

Appendix L

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory G: Traffic Management and

READY ASSET PRO powered by UScellular



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
READY ASSET PRO powered by UScellular
- b. General Application Area
Subcategory G: Traffic Management and Intelligent Transport Systems (ITS)
- c. General capabilities provided
READY ASSET PRO is a LoRa WAN based platform that enables our customers to solve problems, simply. Our end-to-end managed solutions can generate, transfer and optimize data across an endless number of use cases. General transportation solutions currently in play include Parking Optimization, Street Light Control and Pedestrian Counting and Movement.

The intuitive platform allows for detailed reporting on data ranging from space availability to remote streetlight dimming and switching to accurate data on people movement and potential improvement on efficiencies and energy management.
- d. Expected impact on cost/performance/functionality, etc.
Each solution implemented in a Smart City installation is designed to solve common problems facing municipalities. Energy and operational efficiency along with constituent care prove to show immediate data driven savings and optimization.
- e. Subcontractors/partners involved in delivering service
READY ASSET PRO is managed by Ready Wireless and utilizes WMW as its underlying platform. Custom development, dedicated account support and platform management makes the service a leader in the space.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes. Please see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
READY ASSET PRO collects outside data, processes and visualizes it and delivers it to any process, system or person requesting it.
- b. Applicability to government needs
See response to "a" above.

- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use. Provide references

We currently have various end-to-end managed solutions and platforms deployed in over 300 businesses and municipalities. The platform reach is even greater through various channel partners and systems integrators operating in dozens of countries on 4 continents.

Company	Contact	Title	Phone
Home Town Restyling	Tom Casey	Sales Manager, Partner	(319) 350-9636
Baker Group	Mitchell Wood	Fleet Manager	(515) 314-9478
NIFCO	Cory Richards	Account Manager	(402) 310 5751
AG Electric	Barney Grobstick	President	(563) 590-4056

- d. Overall interoperability of turnkey system for government use

READY ASSET PRO operates on an open API platform. Data can either be exported for reporting measures or, with development, the platform can be pointed toward other systems for integration. These efforts would be evaluated under a separate Statement of Work and agreed to mutually before execution.

- e. Accessories available for turnkey offering

READY ASSET PRO has over 120 different connected sensors integrated with the platform and the use cases that those devices address are endless.

In addition to specific device requirements a LoRa gateway for data transport needs to be installed. While the signal range for these gateways is immense, environmental and structural objects may require multiple gateways be put into use.

- f. Thoroughness of the vetting process used to select partners

We go through a rigorous process to determine vendor partners. A team of individuals from various departments evaluate each vendor and determine which vendors will be the best fit. This starts with a demo and based on use cases and scenarios we determine if the vendor can provide the business requirements needed.

- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

For new vendor launches and any enhancements the testing process starts with the use cases that were determined and documented for the release. Each use case will be tested several times from multiple users, from various departments, from the beginning of the process to the end of the process within the Quality Assurance environment. Once all parties approve the launch or enhancements with the Quality Assurance environment, the changes will be pushed to the production environment and tested again by multiple users, from various departments, through the entire process for final approval. During both phases, any issues would be fixed before approval of that phase and then moving onto the next phase.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package. The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
Our Clients provide a specific need, problem or use-case to be monitored with desired outcomes defined. A formal quote specific to those needs is provided for signature.
- b. Project coordination
We procure equipment as needed and work with management or 3rd party to coordinate timing for installation.
- c. Installation and Testing process
Sample devices are sent ahead of project implementation for data integrity and trial purposes.
- d. Client Infrastructure and support assessment process
We assign dedicated account management personnel to the relationship. Our team is available to ensure devices are properly accounted for on the portal, assist with desktop or app support, ensure reporting accuracy and provide ongoing guidance on data trends and actionable items that appear in the platform.

Training sessions are scheduled for different user levels and ongoing support is made available.
- e. End user Acceptance process
Our aim is to ensure the end user is gathering the expected data to drive outcomes whether those efforts are maintenance, performance, location or safety driven. Regular interactions (calls, video conferences) are scheduled to understand and promote acceptance.
- f. Approach to maintenance and support
See response to "d" above.
- g. Initial and Ongoing Training provided
See response to "d" above.
- h. On-going support and enhancement over the life of the agreement
See response to "d" above.

4 - Service Factors:

a. Description of related services included in Turnkey Solution

Embedded in the READY ASSET PRO platform is the framework to develop turnkey solutions for our clients' needs. We can transform and shape the application for whatever the desired target deliveries might be. With the installation of the LoRa gateway, any of the over 120 already built solutions can be quickly deployed and visualized on the same portal.

More and more "things" things will be connected in the future and the application is designed to streamline all device management, basic operations, data aggregations, GeoMapping, reporting and business rules.

b. Experience and qualifications of partners and subcontractors

We have been involved in systems and network integration for 15+ years. Our ability to manage and enable end-to-end solutions is unique in that not only do we have a technical command of the services we put forth, but we support the sales, marketing and ongoing account support effort as well.

c. Description of Additional Integration and Consulting Services provided

In addition to Asset/Sensor Management, we host a number of risk management and performance-based platforms to help organizations solve complicated problems, simply. Other solutions include Broadband Failover, Asset Tracking and Management, Contact Tracing and Social Distance Monitoring through LoRa-based technology, Environmental Controls (temp/humidity), Agricultural Solutions and many more.

IoT Management Services Terms and Conditions

Ready Wireless (“READY”) IoT Additional Terms and Conditions are at www.readywireless.com/terms-and-conditions. (“Additional T&Cs”)

In the event of any conflict between the terms of this Agreement, these IoT Management Services T&Cs set forth below, and the Additional T&Cs, the order of priority (high to low) is Agreement, Additional T&Cs and IoT Management Services T&Cs. Without limiting the foregoing, as provided in the Agreement, (i) Your cellular carrier shall bill and collect the Cellular Services Fees from You (“Subscriber” or “Customer”), and (ii) READY will bill and collect the IoT Management Services Fees.

Introduction. READY will use commercially reasonable efforts to provide Customer with “IoT Management Services” requested by You pursuant to the terms of this Agreement, the Additional T&Cs and the IoT Management Services T&Cs

Definitions. “**Device**” means each unique device provisioned and active on the Customer’s cellular network that allows the transfer of data from a motor vehicle and/or asset to READY’s systems, which device may be provided by READY or a third-party or built into the vehicle or attached to the asset. “**IoT Management Services**” include Real Time Location Tracking, Distracted Driving Behavior and Scoring, Customer Alerts and Notifications, Asset Monitoring, and Vehicle Health and Maintenance. The Services are accessed via the Web referred to as the “Fleet or Connect Portal”.

Device Types for IoT Management Services.

- (a) Customer may purchase Devices that are a true plug-and-play device self-installed by the Customer. Fleet Services for such Devices include real-time location tracking, distracted driving behavior and scoring, vehicle health and maintenance, custom alerts and notifications, fleet portals, account management and custom support.
- (b) Customer may purchase Devices that need to be hardwired in the Customer vehicle. Hardware installation is performed by Customer or your cellular carrier’s preferred vendor. IoT Management Services for such hardwired Devices includes all of the plug-and-play Fleet Services listed above, except vehicle health and maintenance services.

Restrictions on Use of IoT Management Services. READY grants Customer the right to access and use the **IoT Management Services** solely for its internal business purposes while this Agreement remains in effect. No license rights are granted (whether by implied license or otherwise) to Customer except as expressly provided in this Agreement and READY reserves all rights not otherwise expressly granted hereunder. Customer shall not, directly or indirectly, (a) copy, license, sell, redistribute, lease or otherwise transfer or assign the **IoT Management Services**; (b) alter or permit a third party to alter any part of the **IoT Management Services**; (c) use or permit the use of the **IoT Management Services** or any Device in the operation of any service bureau or time share services or for any unlawful purpose; (d) disassemble, decompile, reverse engineer or otherwise attempt to derive source code or other trade secrets from the **IoT Management Services** or any Device. Customer may not use the **IoT Management Services** or Device or provide access to the **IoT Management Services** or Device to any person for any purpose prohibited by law. Customer shall ensure all third parties to which it provides access to the **IoT Management Services** or any Device adhere to the terms of this Agreement. Customer agrees to notify READY immediately in writing in the event any unauthorized access, disclosure, distribution, possession, alteration, transfer, reproduction or use of the IoT Management Services is found.

Data. In the course of providing the **IoT Management Services**, READY may receive or collect data relating to the Customer vehicles and/or assets in which a Device is installed or data related to the owners, operators and occupants of such vehicles and/or assets, including GPS information, vehicle speed, acceleration, hours of operation of the vehicle, vehicle identification number (VIN), vehicle diagnostics information, materials being transported by the vehicle, and information related to employees, contractors and suppliers of Customer (e.g., names and identification numbers of employees and operators of vehicles of Customer) (collectively, “Collected Data”), temperature, performance, capacity, fill rate, volume, and vibration. Customer agrees that while IoT Management Services are provided, and following the termination or expiration of this Agreement, READY will have the right to: (i) use Collected Data in order to provide **IoT Management Services** pursuant to this Agreement, including responding to comments and questions from Customer and implementing the **IoT Management Services**; (ii) use Collected Data to conduct research and development activities, including further developing READY’s services and products; (iii) disclose Collected Data to third parties providing services to READY and permit such third parties to use the

Collected Data in connection with such IoT Management Services;

(iv) disclose Collected Data if required under applicable law, regulation or court order; (v) use and disclose the Collected Data to protect, investigate and deter against fraudulent, unauthorized, or illegal activity; and (vi) use and disclose Collected Data for other purposes so long as the Collected Data is used in an aggregated fashion such that the source of the Collected Data cannot reasonably be identified.

Vehicle-and/or Asset Related Consent. When a Device is installed in a vehicle and/or Asset pursuant to this Agreement, Customer is solely liable to ensure the vehicle is under its authority to receive such Fleet Services.

Security Measures. READY will use commercially acceptable practices to implement technical, administrative, and physical security measures that are designed to protect the **IoT Management** Services from unauthorized access, use or modification. From time to time, READY reviews its security procedures to consider appropriate new technology and methods. However, despite READY's commercially reasonable efforts, no security measures are perfect or impenetrable.

IoT Management Services Area. Customer acknowledges that the **IoT Management** Services are intended and made for exclusive use only within the continental United States. READY makes no representation that the **IoT Management** Services are appropriate or available for use in other locations outside the continental United States. As READY bundles the wireless service within the **IoT Management** Services, Customer may use the wireless service solely in connection with the **IoT Management** Services within such service area of such wireless carrier and will not otherwise misuse the wireless service (e.g., take the vehicle and/or asset outside the carrier service area or insert a SIM card, if applicable, into another device).

Customer Acknowledgements. Customer acknowledges that READY may not be able to provide the **IoT Management** Services at all times due to reasons outside of READY's control, including if: i. the Device and/or Asset is not (A) connected to an appropriate power source or cellular network, (B) transmitting or receiving data or where data functionality is otherwise impaired, or (C) incorrectly installed in the vehicle or is not properly functioning; ii. the Device and/or asset is not active on your cellular carrier's network or there is a failure of cellular networks or any hardware outside the reasonable control of READY; iii. the vehicle operator has manually overridden the functioning of the Device; or iv. the vehicle driver identification function has not yet been completed. Customer may only use a Device with a compatible vehicle and/or asset.

Customer acknowledges that the Device uses a certain amount of current from the battery even when the vehicle is not turned on. Care should be taken in using the Device in vehicles that have old or weak batteries, or that may go extended periods without being started. Customer shall not use the Device or Fleet Services in or with motor vehicles with a modified engine, modified electronic control systems, or cars of any make, model or year that are not supported.

Such use shall be deemed nonconforming and inappropriate use of the **IoT Management** Services and in violation of this Agreement. READY will not be liable for nonconforming and inappropriate use of any Device or **IoT Management** Service. READY, in its sole discretion or at the instruction of the applicable wireless provider, may from time to time make additions to, deletions from or modifications to the **IoT Management** Services and the equipment, software or communications facilities used to provide and receive the **IoT Management** Services. READY shall make commercially reasonable efforts to notify Customer upon adoption of such modifications, except that changes not materially affecting Customer's use of the **IoT Management** Services and minor changes may be adopted without providing Customer with notice to that effect. Continued receipt or use by Customer of the **IoT Management** Services after any modification shall constitute Customer's acceptance of such modification.

READY Portal and License to Use. READY shall make a web portal and related documentation available to Customer for use in connection with the **IoT Management** Services (the "Portal"). READY grants to Customer a non-exclusive, revocable, non-transferable and non-sublicensable right to use the Portal solely for use in connection with the **IoT Management** Services while this Agreement remains in effect solely for Customer's own internal business purposes and subject to Customer's payment of all fees due and payable under the Agreement. The READY Portal and related documentation are Confidential Information of READY (excluding, for clarity, any data or content provided by Customer for use on the READY Portal). Customer shall only permit its authorized employees and agents who have agreed in writing to comply with the terms of this Agreement, to access and use the READY Portal (each an "Authorized User"). Customer shall be responsible for all acts and omissions of any individual who accesses a READY Portal on behalf of Customer or utilizes Customer equipment or who use log-in information provided or made available to Customer by READY. Customer shall promptly (but in any event within twenty-four hours) notify READY of any unauthorized use of a READY Portal or any other known or suspected breach of security related to the READY Portal. All rights of READY and its licensors in intellectual property not expressly granted to Customer are reserved by READY and its licensors. Customer shall cease all use of a READY Portal upon the expiration or termination of this Exhibit or, if applicable, the Phase Out Period. READY will create accounts for a reasonable number of Authorized

Users with a unique user name and password. Customer shall cause Authorized Users to only use these credentials to log in and access the READY Portal in accordance with the requirements of this Agreement. Customer shall be responsible for identifying all of its Authorized Users, for approving access by its Authorized Users to the READY Portal, for controlling against unauthorized access by such Authorized Users, and for maintaining the confidentiality of the user names, passwords and account information for all Authorized Users accounts. Customer shall be responsible and liable for (and READY shall not be responsible or liable for) any activities that occur under Customer's or its Authorized Users' accounts or passwords or as a result of Customer's or Authorized Users' access to the READY Portal, including any actions or omissions by individuals accessing a Customer or Authorized User account without authorization. Furthermore, Customer agrees not to transmit or store infringing, obscene, threatening, libelous, or otherwise unlawful or offensive content or other materials or information that violates the privacy rights of any person or to transmit or store material containing software virus, worms, trojan horses or other harmful computer code or malware when using the READY

Portal. Customer shall abide by all applicable local, state, national and international laws and regulations in connection with Customer's use of the READY Portal, including those related to taxes, data privacy and the transmission of technical or personal data. READY shall not be liable or responsible for the deletion, correction, destruction, damage, loss or failure to store any data or content of Customer located on the Portal. Customer shall be fully responsible for all internet access and connectivity requirements to (and resolving any issues that arise in connection with) access the READY Portal.

Customer acknowledges and agrees that READY owns all right title and interest in and to the READY Portal (excluding, for clarity, any data or content provided by Customer for use on the READY Portal) and any derivative works thereof, and no license to the READY Portal is granted to Customer by implication, estoppel or other than as expressly set forth in this Exhibit. Customer agrees not to: (i) remove or modify any trademark, service mark, copyright or other notice of READY's or its licensors' proprietary rights; (ii) modify, make derivative works of, disassemble, reverse compile, reverse engineer, reproduce, or download any part of the READY Portal, including any software of documentation to which Customer is provided access in connection with the READY Portal; (iii) conduct any benchmark tests or performance tests of the READY Portal without READY's prior written consent and participation; or (iv) sublicense, sell, rent, lease, transfer, assign, distribute, display, disclose, republish, make or permit timesharing or service bureau use or use for any unlawful purpose, or otherwise commercially exploit or make the READY Portal, including any software of documentation to which Customer is provided access in connection with the READY Portal, available to any third party.

Indemnification. In addition to the indemnification set forth in the Additional T&Cs, Customer will defend, indemnify, and hold READY and its affiliates and their respective officers, directors and employees harmless from and against all claims, complaints, losses, costs, and expenses (including reasonable attorneys' fees) (collectively "Claims") asserted by third parties that are not affiliates of READY to the extent arising out of or in connection with (a) the IoT Management Services or any Device (and, for clarity, regardless of whether the IoT Management Services or READY's breach of the Agreement or negligence contributed to such Claims), (b) any libel, slander, or infringement of copyright arising from the material transmitted using the IoT Management Services or any Device; or (c) the combination, integration, or incorporation of the IoT Management Services with a device, product or service not provided by READY. The indemnification procedures set forth in the Additional Terms shall apply with respect to any claim for indemnification under this section.

Notices. All notices and other communications required or permitted hereunder shall be in writing and shall be mailed by certified or registered mail (return receipt requested), or overnight express air courier, charges prepaid, addressed as follows to READY and to the address provided by Customer, and such notices will be deemed to be made when actually received:

READY WIRELESS, LLC
955 Kacena Road, Suite A
Hiawatha, IA 52233
Attention: Legal Department

If to Customer:

COMPANY NAME	
ATTENTION	
ADDRESS	
CITY, STATE	
ZIP	

.

Device Warranty and Refund Policy

READY offers a limited warranty on devices and modules (collectively, the “Device”). If you believe the Device you received is defective, please notify READY as soon as possible and provide sufficient detail to justify your claim. If a Device is determined to be defective in the reasonable discretion of READY, a refund or a replacement (providing stock of the exact make/model/color/condition is available) will be offered if READY is contacted within the specified warranty period noted below.

Please contact your cellular carrier Representative and READY for a RMA # (Return Merchandise Authorization) prior to returning or exchanging any item. Obtaining a RMA# is the only way to ensure a refund or exchange will be processed. You must ship your item within 30 days of receiving your RMA# in order to receive a refund or replacement. Please do not send your purchase back to the manufacturer.

Refunds (if applicable)
Once your return is received and inspected, if approved, your refund will be processed. READY does not offer a refund for the shipping costs incurred upon purchase of the Device. The Device being returned must be received in the same condition as when it left the READY facility. If the returned item is missing any internal stickers or serial number information, a refund will not be issued. Refunds are issued to the same account that the purchase was made from

Exchanges (if applicable)
READY will only replace a Device that is defective, as reasonably determined by READY in its sole discretion. This policy does not apply to breakage caused by Customer negligence or water damage. Once your return is received and inspected, your request will be promptly processed. If there is a problem with your order, please contact READY at 1-800-570-3869 during the below hours of operation:

Monday – Friday 7:30 am to 5:00 PM (CST)

If there seems to be a mechanical, electrical, or programming problem with your Device, DO NOT attempt to repair or try to unlock it yourself or take it to a third party for repair without first contacting READY. Doing so will automatically void any applicable warranty. READY does not reimburse you for third party repairs or purchases. READY shall make all commercially reasonable efforts to ensure that the Device received is as described.

Warranty Term	
Device	Warranty Term
Device (new)	12 Months from ship date to Customer

IOT MANAGEMENT SERVICES AGREEMENT, IoT MANAGEMENT SERVICES TERMS & CONDITIONS, READY’S ADDITIONAL T&CS, AND WARRANTY POLICY ARE ACCEPTED BY CUSTOMER. :

NAME:

TITLE:

SIGNATURE:

DATE:

Appendix N

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

**Subcategory G: Traffic Management and Intelligent Transport
Systems (ITS)**

PARKNAV



NASPO
ValuePoint



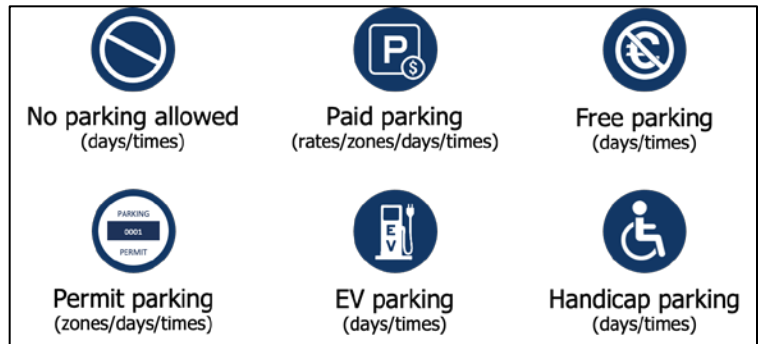
1 - General information:

Please provide a general description of the solution you are offering including:

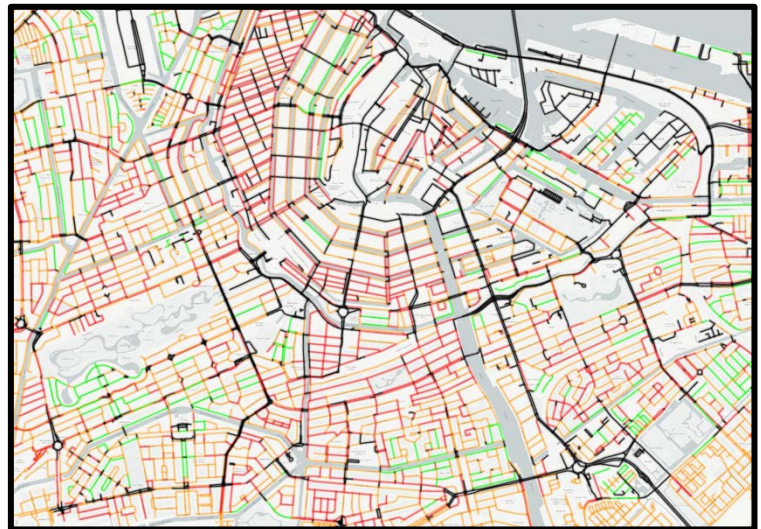
- a. Product Name
PARKNAV Parking Information Service
- b. General Application Area
Subcategory G: Traffic Management and Intelligent Transport Systems (ITS)
- c. General capabilities provided
PARKNAV is a comprehensive parking information service that provides information on the availability of both on-street and off-street parking in a city.

PARKNAV On-street Parking Information services API provides developers with parking restrictions and real-time parking availability.

PARKNAV On-street Parking Restrictions service includes locations, days, times, zones and rates of various curb regulation types on every street throughout a city.



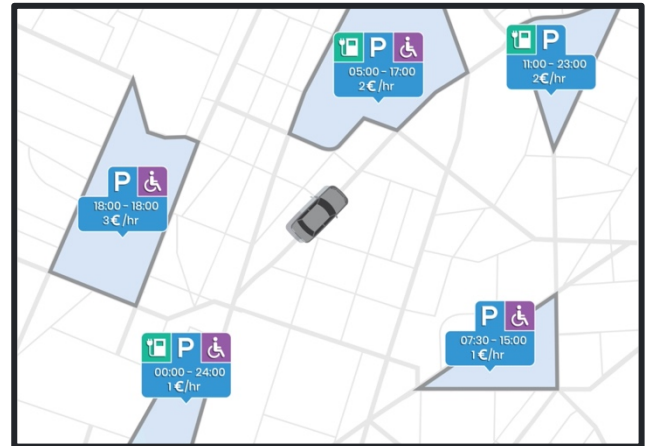
PARKNAV On-Street Parking Availability service uses patented, award-winning machine learning technology to determine most precisely streets that have at least 1 open and legal on-street parking space. This technology has been developed for over 25 years by a globally recognized award-winning data science team to deliver the most accurate real-time parking availability information on the market.



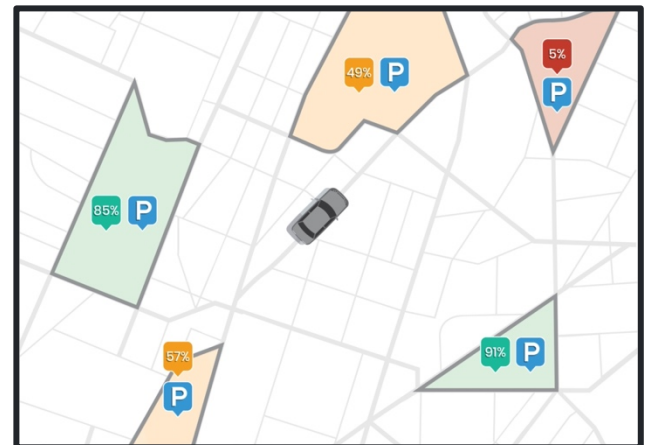
PARKNAV Off-street Parking Information Service provides the locations, space types, days, times, rates, accepted payment methods, number of open spots (based on sensor availability) and other information for outdoor and indoor off-street parking lots and garages. This information is available via our REST API that allows our customers to query for parking lots and garages around a given location, and also get detailed information about a specific parking lot/garage.

Information in our Off-Street Parking Information service includes:

- Restrictions
- Parking gates dimensions or max altitude (including entrance location)
- Total number of parking slots in building/lot
- Availability times/schedule
- Pricing & payment requirements
- Free-of-payment parking lots
- Permit requirements
- Handicap spaces
- Charging stations information
- Off-street Parking Availability

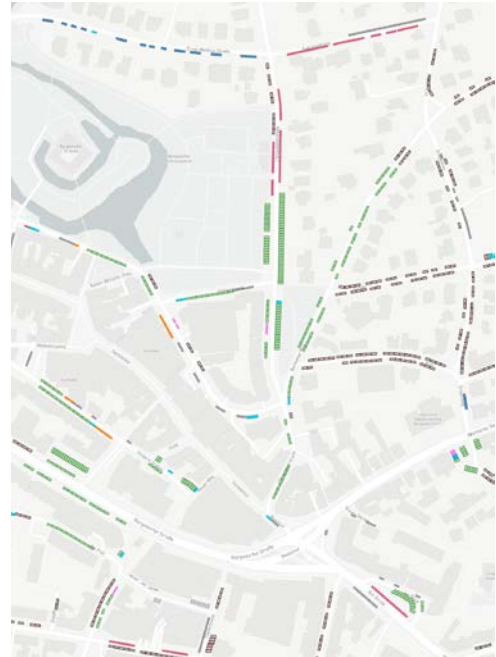


In addition to garage and parking lot locations and their general information, Parknav uses its patented, award-winning machine learning technology to determine, with high precision, the probability of each parking lot/garage having at least one open parking spot. This enables users to determine immediate availability or to plan for future availability. This real-time availability information is updated every minute and is available as part of our API.



PARKNAV City Portal provides detailed analytics and prediction information for all streets throughout a city. In addition to Parknav's on-street and off-street parking information, additional information can be easily integrated into the Smart City Portal to provide users with a single "window" to all relevant smart city information such as:

- Determine the best times to fix potholes
- Determine the best times for street cleaning
- Implement dynamic pricing for parking
- Determine whether to remove/add parking in an area
- Modify the type of parking for a specific area
- Analyze the impact of parking restrictions on traffic flow



d. Expected impact on cost/performance/functionality, etc.

PARKNAV provides city planners with accurate, real-time information on parking through-out the city. With this information, cities can:

- Improve traffic flow and minimize CO2 emissions within the city by routing people more efficiently to available parking
- Have up to date, digitized curbside restriction information including, but not limited to, illegal parking zones, paid parking zones and residential permit parking zones
- Identify areas of opportunity with high/low parking congestion where cities can implement new parking rules
- Completely remove the need for the installation/management/cost/etc. of using ground parking sensors or cameras to identify parking availability
- Provide city parking enforcement with ideal areas of high parking congestion to monitor for parking infractions
- Improve city planning for road construction/maintenance by identifying optimal times on streets where parking congestion is low.
- Increase GDP of high traffic areas by ensuring parking is more efficient for residents and visitors
- Improve city planning for new construction projects (e.g. buildings, hospitals, etc.) to better understand parking needs and the impact these projects will have on parking in the areas surrounding the new construction.

e. Subcontractors/partners involved in delivering service

N/A

f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.

Yes. See attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

a. Strength and functionality of operational product as described

Our PARKNAV parking information service provides real-time information on the availability of on street and off-street parking and parking restrictions to city planners. The strength and uniqueness of our solution includes:

- Parking restrictions are available for 100% of the streets within the city
- Parking availability probabilities for all streets within the city are updated every minute
- Ability to choose between free, paid, and permit parking types
- Parking availability probabilities for parking lots and garages
- Ability to see differing parking types available such as car, bus, truck
- Accurate information on parking facility capacity and pricing
- Information on facility amenities such as EV-Charging, Handicap Parking, etc.
- Works for all mapping platforms (Mapbox, HERE, Google Maps, etc.)
- Easy to integrate JSON/GeoJSON API

b. Applicability to government needs

PARKNAV is a comprehensive service that addresses all the major requirements for use by city planners. Our service includes:

- On-street Parking restrictions for every street in the city coverage area
- On-street Parking availability predictions for every street in the city coverage area
- Off-street parking garage/lot information for 100% of the city coverage area
- Off-street parking availability predictions for all lots and garages in the city coverage area

c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.

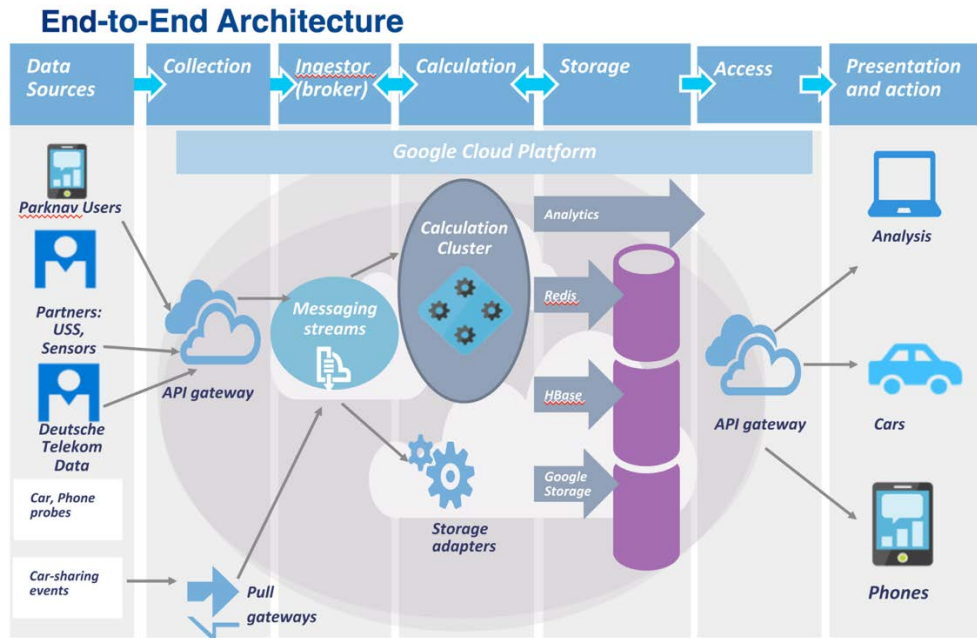
Provide references

PARKNAV is currently available in over 1000 cities in North America and Europe. We have successfully implemented service in Automotive sector with the launch of PARKNAV in BMW vehicles starting 2017. We are also deployed in the telco, oil & gas industry, and public sector. Below are several examples:

- BMW
- Nissan Mobility
- Deutsche-Telekom
- Kuwait Petroleum
- Siemens
- City of Hannover
- City of Bremen

d. Overall interoperability of turnkey system for government use

We deliver PARKNAV service through easy to integrate JSON/GeoJSON API with the architecture shown below:



With this approach, our solution is very easy to integrate and is scalable to support all the needs of NASPO. In addition, we can easily modify our API to address additional requirements that may arise.

e. Accessories available for turnkey offering

In addition to PARKNAV, we offer the following accessories.

- Tools for quality assessment and monitoring.
- Integration support and service.
- Interface (API) implementations as requested.
- Reporting as required.
- Periodical service tests and diagnosis.

f. Thoroughness of the vetting process used to select partners

N/A

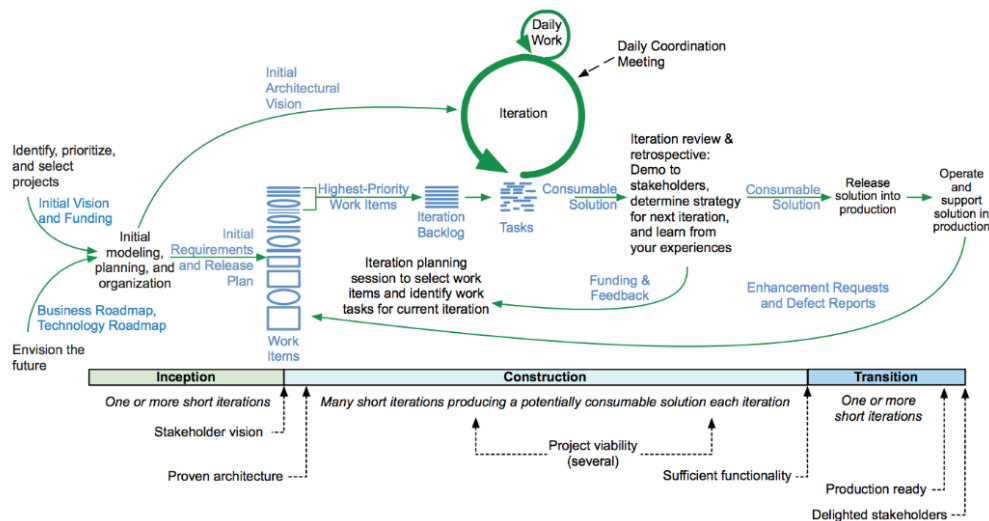
g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

QUALITY MANAGEMENT - Ai Incube adheres to the requirements of Quality Management Systems of ISO 9001:2015 and IATF 16949:2016 and applies the principles of Total Quality Management (TQM). These apply to every position and unit in the organization and is aiming at achieving highest quality for our customers and highest employee satisfaction in our organization.

Our founders' motivations are to better the world driven by leading in innovation while not compromising on safety, security, and reliability. Consequently, we work with our customers to deliver highest quality solutions for their needs together with confidence that if and when issues arise root causes are detected and addressed.

AGILE - Ai Incube uses Disciplined Agile as the core of its development methodology. It borrows heavily from Scrum, XP, UP, Kanban and other Agile methodologies to establish an end-to-end delivery

framework that works well while needing to deliver to customers in a B2B environment. A big emphasis is put on creating working IT solutions that are actually deployed and working in a production environment for customers rather than on simply delivering working software (that still needs to be approved, verified for completeness, deployed, etc.). A high-level overview of the process is shown in the figure below:



3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

a. Pre-installation coordination

Our team will work with your members to finalize the cities to be included and the specific coverage area for each city (e.g., polygons). With this information, our team can begin the process of service activation for each of the included cities.

b. Project coordination

We will assign a Project Manager to plan, implement and deploy our parking information services.

c. Installation and Testing process

Activation of our PARKNAV service for given city includes a comprehensive testing/quality process to ensure information accuracy and precision.

Ai Incube shall maintain two production services (identical copies of each other) for failsafe measures. It would further hold a third, Staging Environment, for testing and approval of improvements postproduction.

For testing/quality, we apply two main methods for quality assessment of the services:

- Manual and semi-manual collection of Ground Truth data
- Automatic tests and monitors

Manual and Semi-Manual Ground Truth Testing

Ai Incube employs its own data collectors who survey the city streets and record ground-truth information about parking availability and restrictions. Data collectors use already existing, proprietary Ai Incube tools that have been perfected to provide most precise and efficient ground-truth testing - enabling efficient, cost-affordable large-scale testing.

Ai Incube also developed camera-processing technologies specialized for on-street parking detection. These tools are now being used to semi-automatically (with human oversight) detect available spots and parking restrictions

Automatic Tests and Monitors

Ai Incube continuously develops and deploys automatic tests as part of its development and deployment process. Such tests include evaluation of software component performance, evaluation of whole-system performance, continuous integration and tests of routine updates of software, and others.

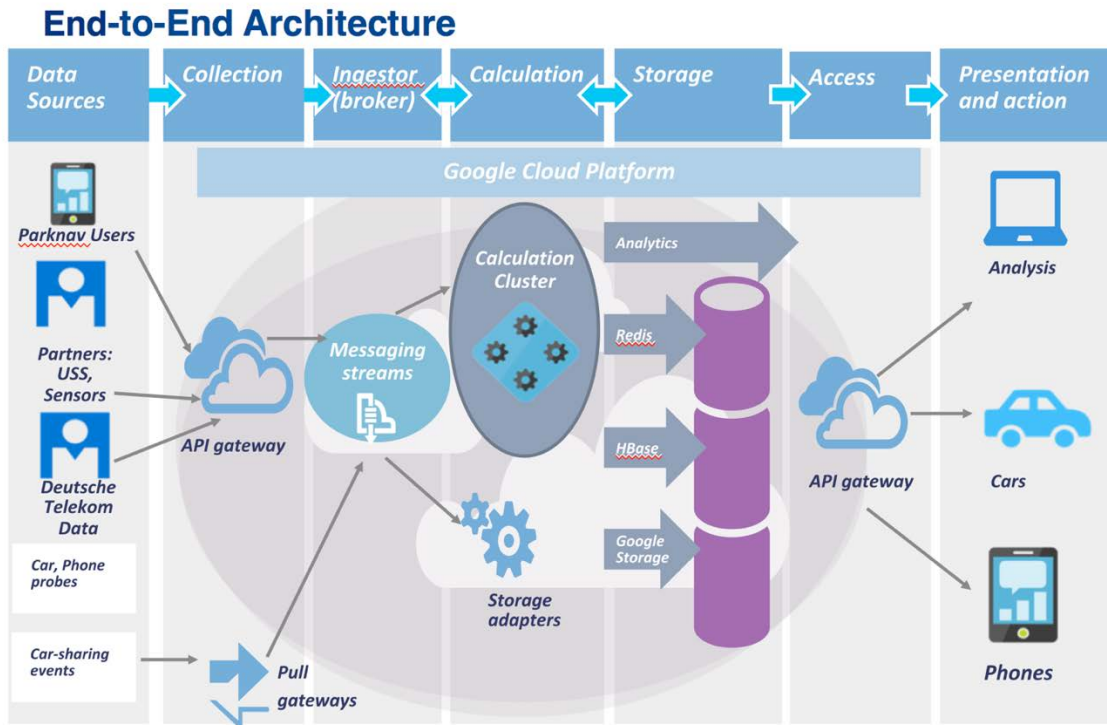
Ai Incube also develops and runs monitors for all incoming data streams, such as floating-car data, mobile-payment data, meter-payment data, and all others. Those monitors ensure that data arrives within specified parameters of frequency and quality as appropriate.

Within our service areas to customers, with our customers' permissions, we also monitor success rates for parking as compared to our models and estimates. While such monitors provide only approximate measurements of our performance, they enable further quality control and early alerts of anomalies.

Ai Incube integrates those monitors into a system that alarms operators if and when any irregularities occur.

d. Client Infrastructure and support assessment process

Ai Incube has scaled Parknav to be able to ingest hundreds of millions of data points per day through its use of Google Cloud Platform. Not only does Parknav rely on Google Cloud Platform to provision the necessary number of computing services on demand and scale with load, it also does not operate any of its services on its own – all of the components of Parknav's infrastructure are operated and supported by Google and come with 99.9% or higher SLAs. This allows Parknav to concentrate on producing the best-in-class parking analysis software without having to maintain, operate and support its extensive infrastructure. With this architecture, there are no specific client infrastructure requirements other than a web-browser and internet access.



e. End user Acceptance process

In order to ensure full customer satisfaction Ai Incube has clear processes on User Acceptance Testing (UAT). Prior to the start of a project a set of predefined KPIs are established which will be used during the UAT to ensure data quality. Ai Incube also assists clients with materials and training on quality assurance.

f. Approach to maintenance and support

Maintenance, support, "bug reporting" and help desk are included as part of the standard SLA included in our license agreement. We will work to ensure a seamless experience for your customer(s).

g. Initial and Ongoing Training provided

As part of the activation of PARKNAV information service, we include workshops and support in the use and structure of our parking service and API's. Detailed API documentation is also available.

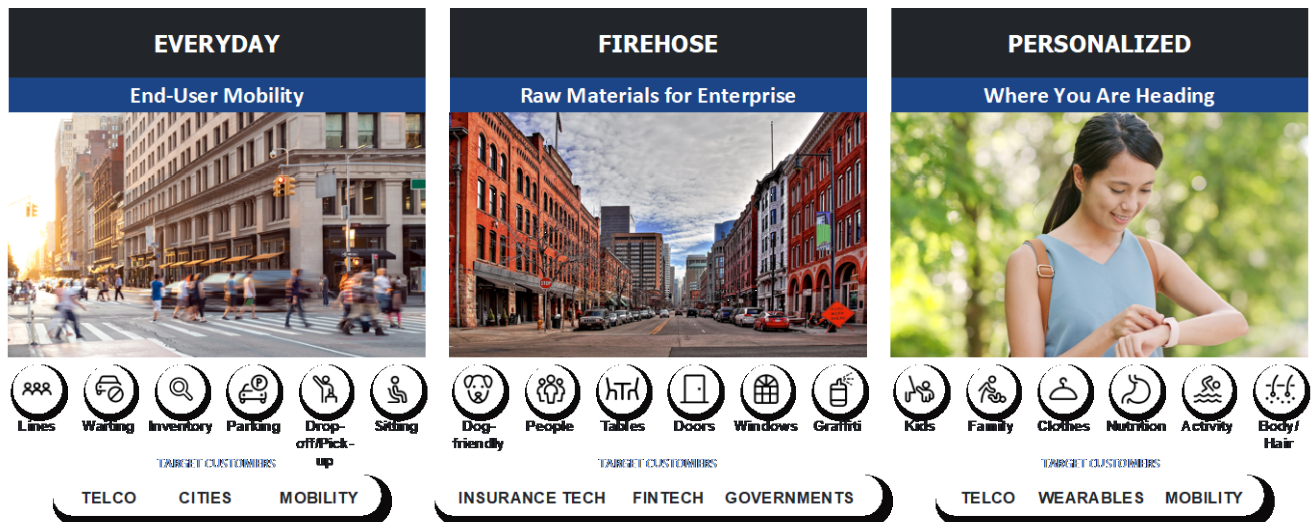
h. On-going support and enhancement over the life of the agreement

We invest heavily in our technology to continually improve the accuracy of our parking information predictions and quality of our data. Enhancements and updates to our technology are provided to our customers via updates as part of our standard licensing agreements.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution

In addition to our PARKNAV parking information service provided as part of this RFP, Ai Incube is continually investing and expanding our portfolio of products to provide on-street predictions for what we call the “live street”. This includes predictions for everyday things impacting end-user mobility, raw materials for cities, and information personalized for consumers. All of these services can be integrated into our City Portal to address specific needs of our customers.



- b. Experience and qualifications of partners and subcontractors

N/A

- c. Description of Additional Integration and Consulting Services provided

Should additional assistance be required in integrating and/or delivering our PARKNAV service, Ai Incube offers consulting services. These services are offered on either a fixed-price or time & material basis. Ai Incube data scientists, artificial intelligence experts, data modelers, app developments, project managers, and IT specialists are available to support specific projects.

Appendix A: End-user License Agreement

DATA LICENSE AGREEMENT

THIS DATA LICENSE AGREEMENT (this "Agreement") is entered into as of _____, 2017 (the "Effective Date"), by and between AI Incube, Inc, a Delaware corporation d/b/a Parknav with principal offices at 222 Merchandise Mart Plaza, Chicago, IL 60654 ("Parknav") and _____, a _____ corporation with principal offices at _____ ("Customer") (each a "Party" and collectively the "Parties").

The Parties agree as follows:

1. DEFINITIONS.

- 1.1 "Data" shall mean the data made available by Parknav to Customer in such reasonable manner as is determined by Parknav, which may include, for example, pursuant to Customer's authorized calls on the PN API or Parknav's sharing of a Dropbox file.
- 1.2 "PN API" shall mean the API Parknav makes available to Customer to enable Data calls, including related documentation, source code, executable applications and other materials made available by Parknav.
- 1.3 "Service" means Parknav's provision of Data to Customer pursuant to the terms hereof.
- 1.4 "Derivative Works" shall mean all analogue, digital or other works that are created from and/or based in any way on the Parknav Data or Archived Data, as the case may be.
- 1.5 "End User" shall mean any entity or person who receives or uses the Archived Data, Derivative Works (of either Parknav Data or Archived Data) and/or HERE Products and Services incorporating the Parknav Data, Archived Data or Derivative Works (of either Parknav Data or Archived Data), for personal use with no right to sublicense.
- 1.6 "Intellectual Property Rights" shall mean patent rights, copyrights, database rights, trademarks, service marks, and any and all other statutory and legal rights and protections available under applicable laws for the protection of intellectual property.

2. LICENSE.

- 2.1 License Grant. Parknav hereby grants Customer a non-exclusive, non-transferable, worldwide license to:
- 2.2 use the Parknav Data including reproducing and/or organizing all or any portion of the Parknav Data and incorporating the Parknav Data with or into the Customer Products and Services;
- 2.3 prepare Derivative Works and market, distribute and license the Parknav Data, Derivative Works and the Customer Products and Services incorporating all or any portion of the Parknav Data and Derivative Works, alone or in combination with any other data, software, products, systems, services and/or applications, directly or indirectly, to End-Users;
- 2.4 evaluate the Parknav Data and Derivative Works, demonstrate the Parknav Data and Derivative Works to prospective customers and develop applications using the Parknav Data and Derivative Works; and
- 2.5 data calls: Customer may call the PN API in order to access the Data pursuant to the PN API definition and keys provided by Parknav to Customer. Customer may request Data through the PN API not more than agreed in writing between the parties

3. TERM AND TERMINATION.

- 3.1 Term. The term of this Agreement shall begin on the Effective Date and automatically terminate on _____
- 3.2 Extension. The term of this Agreement Period may be extended by Parknav for such period as Parknav approves in writing in its sole discretion, upon written request for such extension by Customer.

4. RESTRICTIONS.

Except as expressly authorized by Parknav in writing, Customer shall not: (a) modify or create any derivative works of the Data other than for the Permitted Use; (b) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for the PN API; (c) redistribute, encumber, sell, rent, lease, sublicense, grant access, or otherwise transfer rights to the Data or Service; (d) interfere with, modify or disable any features,

functionality or security controls of the Service or the PN API, defeat, avoid, bypass, remove, deactivate or otherwise circumvent any protection mechanisms for the Service or the PN API; (e) use any Data as an input in models seeking to replicate or extend the coverage of the Data for or in connection with the Permitted Use, (f) embed any Data or Customer's derivatives of the Data in any Customer products, services or systems that would be provided or made available to any third party, or (g) authorize or permit others to do any of the foregoing (collectively, "Prohibited Actions"). Customer will take reasonable measures to prevent the occurrence of any Prohibited Actions. In the event Customer becomes aware of the occurrence of any Prohibited Actions, Customer shall promptly inform Parknav thereof and take measures to stop, and prevent the further occurrence of, any Prohibited Actions.

5. PROPRIETARY RIGHTS. As between the Parties, Parknav retains exclusive ownership of any and all rights, title and interest (including patent rights, copyrights, trade secret rights, and all other intellectual property and proprietary rights throughout the world) in and to the Data, and all copies (by whomever made) thereof. The license does not constitute a sale of the Data, or any portion thereof. Parknav grants no licenses except for the license expressly set forth herein.

6. CONFIDENTIALITY.

6.1. As used herein, the term "Confidential Information" shall mean: (i) for Parknav, the Data, and (ii) for either Party, any and all information, technical data and know-how which such Party (the "Disclosing Party") discloses to the other Party (the "Receiving Party"), which is or may be related to (a) the business, present or future, of the Disclosing Party, (b) the technology or products of the Disclosing Party, (c) the research and development or investigations of the Disclosing Party, (d) the business of any customer of the Disclosing Party, (e) the terms and existence of this Agreement, and (f) any other information which is or should be reasonably understood to be Confidential Information of the Disclosing Party. Confidential Information described in clause (ii) above shall not include information which: (a) is previously rightfully known to the Receiving Party without restriction on disclosure; (b) is or becomes, from no act or failure to act on the part of the Receiving Party, generally known in the relevant industry or public domain; (c) is disclosed to the Receiving Party by a third party as a matter of right and without restriction on disclosure; or (d) is independently developed by the Receiving Party without use of the Confidential Information.

6.2. Each Receiving Party shall at all times, both during the Term and for three (3) years after termination, keep in confidence and disclose to no third party or affiliate of a Receiving Party: (x) any Confidential Information of the Disclosing Party, and (y) in the case of Customer, any of Customer's derivatives of any Data. Each Receiving Party shall protect all such Confidential Information using a standard of care such Party uses with its own information of this nature, but in no event less than reasonable care. The Receiving Party shall not use any Confidential Information other than for the Permitted Use. Without the prior written consent of the Disclosing Party, the Receiving Party shall not disclose any Confidential Information except on a "need to know" basis to an employee of Receiving Party under binding obligations of confidentiality substantially similar to those set forth herein. If a Receiving Party is legally compelled to disclose any of the Disclosing Party's Confidential Information, then, prior to such disclosure, the Receiving Party will (i) assert the confidential nature of the Confidential Information and (ii) cooperate fully with the Disclosing Party in protecting against any such disclosure and/or obtaining a protective order narrowing the scope of such disclosure and/or use of the Confidential Information. In the event such protection is not obtained, the Receiving Party shall disclose the Confidential Information only to the extent necessary to comply with the applicable legal requirements.

6.3. Upon termination of the Evaluation Period Customer shall: (i) immediately destroy and have no further rights with respect to Parknav Confidential Information, including without limitation, all Data and Customer's derivatives thereof, including all copies thereof, and Customer shall provide Parknav with written certification of such destruction, and (ii) have no rights to any Data, derivatives of the Data or knowledge obtained by examining the Data including, without limitation, with respect to the use or development of any Customer products or services.

7. REPRESENTATIONS AND WARRANTIES/RIGHTS RESERVED

- 7.1. Parknav warrants that (a) it has all right, title and ownership, including all Intellectual Property Rights, in and to the Parknav Data necessary to grant the license herein, (b) the Parknav Data does not infringe the Intellectual Property Rights of a third party and (c) the development of the Parknav Data by Parknav and the provision of the Parknav Data by Parknav to Customer hereunder complies with all applicable laws and regulations. Nothing stated herein shall be deemed to grant, transfer, assign or set over unto Customer any right, title, interest or ownership of the Parknav Data, all of which is hereby expressly reserved by Parknav.
- 7.2. Subject to Section 7.1, Customer owns all right, title and interest, including all Intellectual Property Rights, in and to the Customer Products and Services and any Derivative Works. Parknav acknowledges that it shall not acquire any right, title or interest in or to the Customer Products and Services or Derivative Works, based on any use or incorporation of Parknav Data.

8. LIMITATIONS AND LIABILITY OF INDEMNITY

- 8.1. Under no circumstances will either party be liable under any provision of this Agreement, contract, law, statute or other legal or equitable theory for any consequential, indirect, special, punitive or incidental damages, or lost profits.
- 8.2. In no event will the aggregate liability of either party under this Agreement exceed the amount of the license fees paid by Customer to Parknav hereunder.
- 8.3. Notwithstanding anything to the contrary in this Agreement, Parknav shall indemnify and hold harmless Customer from and against any and all claims, actions, liabilities and damages, including costs and attorney's fees, arising out of or in connection with (a) an assertion that the Parknav Data infringes any copyright or other Intellectual Property Right of a third party or (b) any violation by Parknav of any applicable laws or regulations in connection with developing the Parknav Data or providing the Parknav Data to Customer hereunder. The limitations of liability set forth in Sections 8.1 and 8.2 shall not apply to Parknav's indemnification obligations under this Section 8.3.

9. SUCCESSORS AND ASSIGNS

Neither party shall be entitled to assign or otherwise transfer any of its rights or obligations under this Agreement without the prior written consent of the other party, provided that this restriction shall not apply in respect of an assignment by Customer to an Affiliate or an entity that acquires substantially all of Customer's stock, assets or business.

10. NOTICES. Any notice under this Agreement shall be sent to the individuals at the address identified below.

For Customer:

Name: _____

Title: _____

Email: _____

For Parknav:

Name: Eyal Amir

Title: CEO, Parknav

Email: eyal@parknav.com

9. GENERAL PROVISIONS.

- 9.1. Entire Agreement. This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof, and supersedes all prior agreements, understandings and communications between the Parties with respect to such subject matter. No modification or amendment to this Agreement shall be effective unless in writing and executed by a duly authorized representative of each Party.
- 9.2. Choice of Law; Jurisdiction. This Agreement is made under and shall be governed by and construed in accordance with the laws of the State of Delaware and specifically excluding from application to this Agreement that law known as the United Nations Convention on Contracts for the International Sale of Goods.
- 9.3. Assignment. Neither Party shall assign or transfer any rights or obligations under this Agreement without the prior written consent of the other Party.
- 9.4. Partial Invalidity; Waiver. If any provision in this Agreement should be held illegal or unenforceable by a court having jurisdiction, such provision shall be modified to the extent necessary to render it enforceable without losing its intent, or severed from this Agreement if no such modification is possible, and other provisions of this Agreement shall remain in full force and effect. A waiver by either Party of any term or condition of this Agreement or any breach thereof, in any one instance, shall not waive such term or condition or any subsequent breach thereof.
- 9.5. Force Majeure. Neither Party shall be in default or be liable for any delay, failure in performance (excepting the obligation to pay) or interruption of service resulting directly or indirectly from any cause beyond its reasonable control.
- 9.6. Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original, and both together shall constitute one and the same document and such original signatures may be delivered to the other Party by facsimile transmission or by email.

IN WITNESS WHEREOF, the undersigned representatives of the Parties have executed this Agreement or have caused this Agreement to be executed on their behalf, as of the Effective Date.

AI Incube, Inc. d/b/a Parknav _____.

By: _____

By: _____

Print Name:

Print Name: _____

Title:

Title: _____

Date: _____ 2017

Date: _____, 2017

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory G: Traffic Management and Intelligent Transport Systems (ITS)

Subcategory P: Health and Human Services

Client Company name:	Home Town Restyling
Client name of contact:	Tom Casey
Client contact title:	President
Client is a daily user, occasional user, etc.:	Daily

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Fred Haumesser no later than Friday, November 18th.

Thank you for your assistance in this process.

- 1. For what services do you use USCC's product, and how long have you been USCC's customer?**
Ready Wireless Fleet management services, 1 year
- 2. Would you recommend USCC to other customers? Why?**
Yes, the quality of the product has been exceptional. When we have had questions on how to utilize the platform their team has been timely, knowledgeable and friendly.
- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services?**

They had a rollout meeting with us to describe the process. We found it remarkably easy to implement. Installation was quick and painless.

- 4. How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

They have always been timely. Can't think of an incident where it took a longer than expected response time.

- 5. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

They have not disappointed us in any areas.

- 6. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

Yes. It has exceeded expectations and has been very useful for our business.

- 7. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

Wish they had an alert for red light and speeding cameras.

- 8. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

We have been extremely satisfied all the way around with them. Great team. Great service. Great product.

- 9. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

None

Appendix O

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory H: Snow & Ice Removal and Route Management

SkyHawk Telematics



1 - General information:

a. Product Name

SkyHawk Telematics

b. General Application Area

Subcategory H: Snow & Ice Removal and Route Management

c. General capabilities provided

SkyHawk's ConnectAnywhere web-based monitoring solution, which is hosted out of the AWS Data Centre, guarantees 99.9% service availability, 24/7 onsite support, automated system monitoring and dynamic resource allocation controls. For instance, as more network bandwidth, CPU, RAM, and storage are required, the system dedicates the necessary computing resources. Furthermore, the solution provides a separate, dedicated database, virtual server, IP address and SSL security. These dedicated resources ensure the highest level of performance and guarantee that the system is not degraded by other companies sharing the same system resources.

ConnectAnywhere allows unlimited user accounts or logins with Skyhawk staff providing the initial account setup and administration. Once the system is fully operational, clients have complete administrative IT access to the features and functionality of the system. The ConnectAnywhere solution provides complete GIS mapping integration and interface capabilities to other client software applications with REST API.

Some key features of the SkyHawk solution Include:

- Integration with multiple spreader controller systems that delivers the ability to accurately monitor & report on winter material usage and related cost.
- Ability to connect to multiple inputs, including PTO systems allowing the monitoring and reporting of plow position.
- The ability to obtain ECM engine data including fuel efficiency characteristics such as: Total Fuel Used (L), Fuel Rate (L/h), Instantaneous Fuel Economy (km/L), Average Fuel Economy (km/L) when available from the vehicle manufacturer.
- The ability to report on unsafe driver actions such as speeding (with local speed zone), harsh braking, harsh acceleration, etc.
- Alerts and alarms that are configurable and which can be delivered directly to users via email or SMS messaging.
- Unlimited number of user accounts (usernames and passwords) with complete administrator-level access and system control, multiple user access levels (e.g., Viewer, Manager, Admin, etc.) which are controlled by the administrator.
- The ability to create email and text contact lists per asset for real-time notifications
- Map options default to Google, but access to client maps is available via an ESRI/GIS link.
- The website is protected with an industry- standard, 128-bit encryption with an SSL certificate, providing the ability to filter vehicles in real-time as well as the view of the data online.
- Custom Geo-Fencing and alerts on activity in and out of Geo-Fenced areas including Zoom-In, Zoom-Out, Pan, Drag- Zoom, Road Map Data, Air-Photo Data, etc. Access all reports in real-time online.
- Optional - Tablet support for in- cabin operations supporting advanced navigation and routing options.
- Optional - A completely integrated satellite asset tracking option for vehicles and for high-valued, non-powered assets.

Our solution can integrate with other software and IT applications and is built on one of the most advanced networks and computing platforms available, providing a long-term solution to our customers. Thus, our telematics solution will meet, and in many cases exceed, all aspects and requirements of the organization.

The SkyHawk solution is provided to our clients as a monthly online service, not as "Software" in the traditional sense. Customers will not have to install any programs, routines, scripts, etc. or run any software to use the SkyHawk ConnectAnywhere solution. All you need is a modern browser and internet connection.

SkyHawk Telematics is device-agnostic. We pick the best hardware manufacturers from around the globe to address each vehicle type requirement, from simple track-and-trace, to complex integrations, to vehicles with multiple IO requirements.

Each piece of hardware is selected to perfectly fit each vehicle's specific requirements, and not one piece of hardware is made to fit all. Partnering with multiple hardware vendors also means that we are able to offer our clients the most current and up-to-date hardware, ensuring that we future proof your solution by not only meeting the requirements of today, but are also flexible enough to anticipate and meet future requirements.

The modems we offer have a robust set of features with reliable track records, including standard store- and-forward capabilities for when the vehicle is out of cellular coverage, as well as the ability to receive and perform over-the-air (OTA) configuration or firmware updates in the field. This eliminates the need to physically visit the vehicle for support and maintenance.

SkyHawk's most widely used modems range from simple track and trace, to the most complex applications, used for optimal winter maintenance tracking.

d. Expected impact on cost/performance/functionality, etc.

We are proud to join our strengths in delivering industry-leading and secure, Internet-based GPS tracking and management solutions to Power Utility organizations and advanced work truck sectors.

SkyHawk helps our state and municipal clients to:

1. **Reduce costs** (fleet size/utilization, fuel/materials usage, maintenance, theft reduction, etc.)
2. **Increase productivity** (route optimization, improve service levels, remote monitoring, vehicle WiFi hotspots, incident responses, in-field information access, dispatch, etc.)
3. **Improve safety** (improved driving behavior (speed/harsh events), accident alerts, hours of service/ELD, risk reporting, etc.)
4. **Reduce environmental impact** (monitor salt/chloride usage in environmentally sensitive areas, reduce CO² emissions, automatic GHG/carbon footprint reporting etc.)

We do this using ConnectAnywhere™, our advanced cloud-based monitoring system, coupled with our suite of in-field data collection devices and applications. Our solution gives our clients detailed, real-time and historical data required to make the best operational and management decisions.

Our solutions are currently installed in over 10,000 vehicles government and winter operations vehicles across North America.

e. Subcontractors/partners involved in delivering service

For the purposes of this submission there are no subcontractors or partners required to deliver SkyHawk's service. If, as determined by the scope of work of each opportunity or client engagement, there is a requirement to work with or use contractors/partners, SkyHawk has the capability and capacity to do so. We have done so on multiple projects to date, as needed.

f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.

Yes. See attached End User License Agreement (EULA)

2 - Turnkey Wireless Solutions:

- a. Strength and functionality of operational product as described

SkyHawk's ConnectAnywhere solution is a core platform used to offer our clients full oversight of their mixed fleets, assets and the underlying technology used to track, monitor and maintain core services that people depend on daily.

SkyHawk's Winter Operations GPS fleet management solution is unique in the industry, supporting a wide range of spreader controllers and sensors, and includes specialized winter ops reports. The solution effectively and efficiently deploys, monitors and manages fleets, drivers, assets and material usage.

Winter Operations managers have real-time and up to date visibility on the performance of drivers, the current state of snow removal, as well as other sources of information necessary to monitor overall operating costs, spreading frequency, and quantities to improve environmental and performance metrics.

Winter Operations is the functionality that makes SkyHawk's Fleet Tracking platform stand out from the pack.

The SkyHawk solution integrates with a wide variety of computerized spreader controllers, and, whenever possible, pulls the actual material values from the controller itself, rather than performing a calculation-based estimate.

ConnectAnywhere then has a wide variety of powerful Winter Operations reports available.

Hardware Highlights:	
SkyHawk's hardware modems are non-proprietary and can be implemented on multiple AVL systems.	
Modems have a 3-axis accelerometer to detect and indicate harsh acceleration and braking events in real time .	
Modems have onboard, non-volatile, permanent memory capable of storing a minimum of one month's worth of data . In situations where communication is lost or interrupted, the collected data is stored and transmitted immediately once communication has been re-established by entering an area with cell coverage.	
Modems report real-time events such as: ignition on/off, I/O state changes, harsh events, excess RPM and speed, etc.; reporting frequency can be every 1 second while moving or stopped and every 15-degree change in GPS heading. [Recommended default of 15 second reporting]	
Hardware use true GPS signals for position and does not use assisted GPS positioning off of cellular triangulation.	
Hardware is remotely configurable over-the-air	
SkyHawk offers modems that operate on the 4G LTE networks with 3G fall back with data transmission via TCP/IP connections.	
Hardware is:	
- powered by the vehicle's ECM data port (including OBDII, J-1939 Type 1/Type 2, and J1708), or the powered by the vehicle's electrical system in such cases where an ECM port is unavailable - designed to withstand typical power surges that may occur within a vehicle's electrical system - operates on 6 to 36 volts with no voltage regulator or converter added to the power line	
Modems have Wi-Fi and Bluetooth wireless connections. Wi-Fi provides Internet access via cellular data connection. Wi-Fi is configurable with defined SSIDs and passwords. Wi-Fi is also configurable to not broadcast SSID.	
Modems have the options of being installed within a tamper proof case.	
Modems collect and transmit data from a growing range of spreader control systems	

Modems tracking of blade position using one or a combination of Plow Blade Proximity Sensor, Hydraulic Pressure Sensor and IONS Electric/Air Over Hydraulic Sensor to ensure clients get accurate plow positing reporting.
ECM cables are direct cabling with no 3rd party hardware inline between the AVL modem and the vehicle ECM port. Connects to OBDII, J-1939 Type 1/Type 2, and J1708.
Modem operating temperatures from -22°F to +158°F with a humidity of 95%.
Wireless Capabilities: Certified on all major carriers (AT&T, Verizon, US Cellular, Sprint). Modems can utilize different cellular carriers, depending on the region, to provide the best available coverage for the entire fleet.
Select Modems interface with IP enabled dash cameras to provide image transfer to ConnectAnywhere.
Select modems utilize a windshield mountable GPS and communications antenna to reduce tampering. All antennas and cables are suitable for simple and permanent vehicle mounting without affecting other vehicle components or operating systems.
SkyHawk offers modems that have a backup battery used for detection of loss of GPS or power. ConnectAnywhere software can send alerts via SMS and email to selected contacts when tampering is detected.
Cloud Based Application: ConnectAnywhere
ConnectAnywhere software utilizes Google Maps as its base mapping view and is officially licensed as SkyHawk is a certified Google partner . ConnectAnywhere also has a search function to easily find vehicles, assets, geofences, and landmarks . Maps can be viewed as Satellite, Terrain, Hybrid, and Street Level. Also tracking provides a breadcrumb trail showing each timestamped movement of the vehicles.
ConnectAnywhere is a secure cloud web-based solution for remote configuration, management and update series for the maintenance of GPS telematics. Vehicle positions and status automatically update on screen without any input from the end-user.
Asset tracking data is not routed through any country other than Canada, and the cloud-based servers are physically located in USA.
ConnectAnywhere has a complete screen refresh within 15 seconds and generates reports within 3 minutes for an end-user using any modern Internet capable device and web browser.
End-user system access is available 24/7 (24 hours 7 days a week) via any web browser connected to the Internet
The system is capable of showing, in real time, the Automatic Salt Control (ASC) data , as well as generate suitable reports based on available spreaders. This data includes such things as set/actual rates, total material dispensed as well as trip and/or seasonal totals.
ConnectAnywhere has the ability to organize vehicles, employees and users in a multi-tier organization . It offers the ability to report performance metrics rolled-up at different hierarchical levels and the ability to drill-down and across the hierarchy to investigate trends and anomalies .
ConnectAnywhere supports user-configurable vehicle identification .
Information data stored by the SkyHawk is accessible on-line for a period of up to two years and maintained in a data warehouse beyond two years. Data is accessible by request for a minimum of 7 years or the lifetime of the contract (whichever period is longer) without additional cost. Data older than 7 years shall be made available by request on compatible data storage devices. The maximum latency period between the most recently collected data and the time that it is entered into the data warehousing system is no more than 30 seconds and no more than the normal latency afforded by the network being used.
Geofences can be created within ConnectAnywhere via a simple drawing tool. Geofences can be assigned to specific vehicles or the entire fleet. Geofences can also be public or private to specific users. Alerts can be set up to notify users upon an asset entering/exiting geofences . Finally, specific geofences can be setup as “Storage Depots” wherein <u>salt that is offloaded from the spreader is not included in our salt reports</u> , allowing the users to have an accurate reflection of the amount of salt dispersed on the roadways over a specified period of time

Data is backed up daily.
ConnectAnywhere provides an unlimited number of user accounts and contacts (i.e. <u>no “per user license”</u>).
ConnectAnywhere has the ability to track up to 10,000 vehicles in real-time , with all vehicles viewed at the same time.
ConnectAnywhere utilizes SSL (Secure Socket Layer) internet security (i.e. accessible via https).
ConnectAnywhere is not limited to a specific browser or version (Google Chrome, Internet Explorer, Safari, Firefox, etc.).
ConnectAnywhere supports GIS/ESRI data and application integration and mapping with the ESRI connection such that maps can either be hosted, or preferably, linked to the client’s ESRI database so that when changes are made, they are made on the mapping platform for the AVL at the same time.
ConnectAnywhere has end user full administrator rights for: • Adding/editing user accounts and asset contacts • Easily managing account privileges and profiles across all user groups • Input/output configuration and labeling • Hardware setup and management for AVL, satellite asset tracking and lone worker/personnel tracking • Complete asset management including renaming, hardware and contact assignments.
ConnectAnywhere has the ability to create and manage public and private geofences .
ConnectAnywhere has the ability to integrate with client or third-party server infrastructure to extract and display photos and/or video captured by a dash camera within a vehicle.
The primary display of ConnectAnywhere is a computerized map view in real time of the entire fleet and the most recently communicated status of vehicles. The map includes highway identifiers including other linking roads. Vehicle icons rotate to display proper movements and direction of travel .
ConnectAnywhere has the ability to incorporate weather data into the map layer from client’s contracted weather services vendor.
ConnectAnywhere can display tracings of the vehicle movements in real-time on the road map; this map accurately represents the department’s base map and any other significant geographical features.
ConnectAnywhere provides scheduled reports to be delivered at user-defined intervals and formats.
Reports are printable and can be exportable into Excel and PDF reports. Please see Appendix for samples of the reports available.
A public access site can be created and customized for public viewing - to allow citizen tracking (read-only map displaying vehicles in real-time or with a lag for safety reasons)
Ability to deploy portable devices for GPS tracking of contractors and rental equipment
SkyHawk provides seasonal deactivation for units that are not in use wherein no carrier fees are charged, and the ConnectAnywhere fee is reduced to a suspension fee.
ConnectAnywhere Reports:
SkyHawk’s ConnectAnywhere standard reports include: History Report, Materials Admin Setup, Vehicle Trip Report, Fleet Status Report, Vehicle Detail Report, Long Term Parking Report, Inputs Report, Spreading by Speeding Report, Harsh Events Report, Speeding Report, Input Based Speeding Report, Geofence by Vehicle Report, Geofence by Geofence Report, Route Activity Report, Winter Operations Trip Report, Route Service Report, DLA Report, Malfunction Indicator Light, Winter Operations Material by Time Report, Winter Operations Material by Geofence Report, Sweeper by Geofence Report, Dust Control Report, Fleet Utilization Report, Non- Productive Idle Report. Please see Appendix for samples of the reports available.

The Route Activity report displays routes, the portion of a route, or combination of routes, that has been plowed, had material applied, travelled, swept, or has had a combination of these attributes completed (i.e. which roads have been both plowed and salted). Users can run the report for current or historical data. Roads that are completed are color coded, the color fades with time, to show white if the road had been completed over the designated time interval. Routes can be directional. This report also shows the percentage of the route that has been completed over the selected time interval.
The Winter Operations by Trip report displays the amount of material dispersed by a vehicle over a given period of time. (Note: The end of the trip material offloaded at the depot from the spreader vehicle is not included).
The Material by Time report shows the operational costs, labor costs, fuel costs and material costs incurred over a winter event across the entire fleet of vehicles.
The Route Service report shows the streets that have been plowed and the streets that have had material applied over a live map view.
The Input Speeding Report shows events where a vehicle has exceeded a selected speed when an input such as a plow is down, or sweeper broom is on.
The Material Speeding report shows events where a vehicle has exceeded a selected speed when a spreader is dispersing material.
ConnectAnywhere has a Fleet Utilization report for all vehicles within a fleet, showing the engine hours, odometer, the amount of fuel used, the run time, and idling time.
The Malfunction Indicator Light (MIL) report shows all active ECM trouble codes across the fleet of vehicles.

b. Applicability to government needs

SkyHawk has delivered advanced telematics solutions to the mixed fleet, including winter operations functionality, for more than 7 years to clients in the USA and Canada. Our continued focus on being the industry leader in this sector and in working with our clients has produced functionality which includes:

- integration with most major material spreader controllers,
- cost-based reporting for material usage,
- winter operations trip & material usage reports,
- public winter ops site,
- in-cab route optimization,
- route navigation and return-to-route,
- route activity reporting,
- blade wear report,
- spreader speeding,
- direct liquid application (DLA) report, and much more.

As an end-to-end solutions provider, with a proven track record of successful client partnerships, we understand the needs of complex deployments such as those defined by the State of Utah. As such, we are fully committed and confident in our ability to provide a solution that not only meets but exceeds the goals, objectives and responsibilities that would come with this relationship. To support our belief in that ability, below are some components that we feel fully support the project scope as defined in this RFP.

Experienced and competent subject matter experts: SkyHawk has a team that has successfully delivered similar projects of scope and scale. SkyHawk's team includes senior management/corporate project sponsors, sales account managers,

project management specialists, operations/procurement/order fulfillment staff, installation teams, support staff, and financial/billing specialists.

Project Management: Effective management is vital to the overall success of any project and SkyHawk has proven its ability to deliver telematics projects to complete vehicle and feature roll with very large and complex projects.

Project Management Approach

Skyhawk's Project Team utilizes the Project Management Institutes (PMI) project methodology phased approach that is broken down into five (5) process groups: Initiate, Plan, Execute, Monitor and Close. In each process area, we have identified key documents and tools to serve as inputs that result in deliverables for each phase.

SkyHawk's project team will spend a considerable amount of effort on detailed requirements gathering to ensure a complete understanding of the organization's needs and will compile a comprehensive Project Plan which we feel is critical to the project's success. The Project Plan will be updated regularly as the project progresses, and will establish project roles and responsibilities, a detailed schedule of tasks, Quality Plan, risks, and Change Control. Additionally, SkyHawk's project team will work with your project team in preparing a full updated project schedule, including the installation schedule. Bi-weekly status meetings will be held to review the project schedule and to review any open issues in SkyHawk's JIRA ticketing system.

Project Communication

Project Communication can be established in the form of regularly scheduled project meetings with status reports issued weekly. The status report will contain at a minimum the following information:

1. Dashboard view on the progress of installations, tracking completed installs to planned
2. Task / Action Item List from previous meetings
3. Defect /Issue Log generated from the Jira Ticketing System
4. In addition, SkyHawk will collaborate with ODTO on preparing awareness communications for ConnectAnywhere training, hardware installation training, etc., as appropriate.

Communication Plan

The Project Communication plan will be created in partnership with SkyHawk and the State's Project Managers to outline how the AVL project team will be communicated during the project.

The Communication Plan shall be completed early enough in the project to be included for review at the Project Kick-off Meeting. Communications include but not limited to; status, meetings, issues, deliverables access, and design/document reviews.

Reporting Methods

SkyHawk, in collaboration with the State's project team, shall determine reporting and communication cadences. During the project implementation phase, the Status Report will be issued weekly or bi-weekly, prior to the Project Team Meeting. The Status Report will contain percentage complete and dashboard views of scope, schedule, cost, and quality. It will be prepared in formats approved and will contain at a minimum the following information:

1. Progress Dashboard showing percentage complete from previous meetings
2. Defect Log generated from the Jira Ticketing System
3. Project Status as it relates to the Work Plan
4. Deliverables status
5. Planned activities for the upcoming two (2) week period
6. Future activities
7. Requirements Traceability Matrix (RTM)
8. Report and remedies in case of falling behind Schedule
9. User Acceptance Test Feedback
10. Risk/Action/Issues/Decision (RAID) Log

Solution Configuration

SkyHawk's "ConnectAnywhere" solution is the result of our unwavering commitment to our client partners to provide them the data they require to make informed decisions to maximize operational efficiency, minimize environmental impacts, and protect the safety of both employees as well as the general public. Through continual consultations with the people responsible for the wellbeing of municipal, provincial, and state fleets and the roadways on which they operate, we have incorporated the feedback of these industry experts, along with the lessons we have learned along the way, to the data we collect and the information we report.

To accommodate the ever-increasing volume and diversity of data sources we pull from, the latest version of ConnectAnywhere is architected using modern design techniques that allow us to support many thousand simultaneous connections while maintaining flexibility. This provides us the capability to add or modify the underlying data of ConnectAnywhere to support new feature development without the complexity and downtime that would be required in a more traditional relational database environment.

This flexibility also allows us to support a wide variety of data collection devices, including multiple models of spreader controllers, telematics modems, asset trackers, etc. which enable us to provide a "right-sized" solution for the highly diverse fleets our clients maintain. We also promote "configuration" over "customization"; when we are presented with a business problem to address for one of our client partners, we approach the solution in such a way to benefit all of our users, with consultations as necessary, and make the additions available to our entire client base with the capability to adjust parameters to suit their own operational needs

The client onboarding process involves our project team gaining a thorough understanding of your business requirements, which is then used in the setup of your ConnectAnywhere portal. Starting with the master vehicle list, we meticulously review every vehicle and the data points to be collected from each, including such items as the ECM type, spreader controller, discrete inputs for plow blade position or beacon light monitoring, etc. This is then entered into ConnectAnywhere, which allows us to normalize the potentially many different sources into the consistent user experience in terms of display and reporting. From there, we can adjust the vehicle messaging profile and event thresholds to suit your business goals.

We also work with you to gather the user account information to create the "account templates" that control the functionality and subset of assets that each end-user has available to them. Other key configuration items include the setup of system alerts and scheduled reports.

Specialized Solution Offering: When dealing with a complex fleet of mixed vehicles with specialized reporting functionality (e.g. winter operations) it is very important to acquire a solution that is designed and built for the vehicle types and operations of a large municipal organization.

SkyHawk's ConnectAnywhere telematics solution has been designed and built specifically for this application and supports the specialized and advanced functionality required to more effectively and efficiently operate the services of your organization.

Vendor solution engineering/customization: While having specialized and feature matched system functionality is very important it is also important to have a telematics vendor that has the resources and capabilities to perform solution engineering. Your organization may likely have requests and requirements which need custom development and attention to properly integrate with existing technologies and systems, including data exchange with other software applications. This cannot be achieved with "out-of-the-box" functionality.

SkyHawk has a team of solution specialists and software engineers that are capable of performing such tasks. Your organization will have direct access to the Company who owns, designs and develops the solution and NOT a solution reseller.

Installation Plan/Staff: Vehicle installations and testing are one of the most critical parts of any telematics system. At SkyHawk we refer to it as the "foundation" upon which all other functionality is built or layered. A well-designed installation plan along with a team of reliable installers is required for success.

Furthermore, it has been the experience of SkyHawk that best results are achieved when a combined approach of vendor/contracted installers working in conjunction with the City's mechanics and technical staff is utilized.

Effective Communications Plan: Engagement of your staff and departments to obtain a deep understanding of goals and objectives, as well as obtaining input, feedback, and required "buy-in" from management, system users and stakeholders leads to a better managed and implemented solution. This is best accomplished with an effective communication and engagement plan which starts before implementation begins and carries through all project phases.

SkyHawk has significant and relevant experience working with large clients in delivering successful communication plans. Our Project Team is built of experts in the deployment of AVL projects. They are motivated by excellence and have the combined skills and capabilities to deliver the project on time and on budget and of the highest quality.

c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.

Provide references

SkyHawk attributes a significant portion of our success to the belief that our client relationship is a true partnership. We take a proactive approach to work with our clients and they have been instrumental in the design of our solutions. Our clients motivate and challenge us to constantly seek to develop and refine our technology. As we continue to grow and expand, SkyHawk will continue to seek input from our clients to allow us to continue to advance the telematics industry with innovative solutions. Additionally, SkyHawk remains committed to providing a high level of service throughout every layer of every project.

The SkyHawk client size ranges from enterprises account to small municipal governments. Our solution is currently installed in +5,000 vehicles for Hydro One Networks Inc, +900 vehicles for the Iowa Department of Transportation, +900 vehicles for Nova Scotia Department of Transportation, currently rolling out 10,000 units with Hydro Quebec.

The following are a sampling of some governments clients that currently use the SkyHawk solution:

City of Portland, MA	North Dakota DOT
Town of Davenport, IO	Nova Scotia DOT
Town Urbandale, IO	County of Grande Prairie, AB
Rochester Hills, MI	City of Red Deer, AB
Midland County, MI	Federated Co-op, SK
Muskegon CRC, MI	Manitoba Hydro, MB
Midland CRC, MI	City of Hamilton, ON
City of St Clair Shores, MI	Hydro One Networks, ON
City of Kalamazoo, MI	Town of Flat Rock, NL
Stark County, OH	Hydro One Networks Inc., ON
The city of Brunswick, OH	Municipality of Chatham-Kent, ON
City of Joliet, IL	Hydro-Quebec, PQ
City of Springfield, MO	Town of Quispamsis, NB
City of West Fargo, ND	Town of Rothesay, NB
City of Pittsburgh, PA	Town of Dieppe, NB
City of Mount Pearl, NL	Portugal Cove-St. Philips, NL

Our references below will attest to SkyHawk's ability to deliver a superior product on time and in scope.

Reference (1)

New Hampshire Department of Transportation

7 Hazen Drive Concord, New Hampshire 03302-0483

David Gray

Winter Maintenance Program Specialist

(603) 485-3806 ext. 324

dgray@dot.state.nh.us

October 2016

Ongoing Project

GPS/AVL Winter Operations Solution. 65 Winter Operation Vehicles, and 24 Pickup Trucks - 89 Units

\$272,072.66

Reference (2)

City of Pittsburgh

414 Grant St. Pittsburgh, PA 15219

Chris Belasco

Project Manager

(412) 400-4505

chris.belasco@pittsburghpa.gov

October 2018

Ongoing Project

Complete Telematics Solution, Route Optimization, and Route Navigation system. 138 winter vehicles with a mix of approx.

350 heavy and light-duty vehicles - 488 Units

\$1.5 Million

Reference (3)

City of Hamilton

71 Main Street West, Hamilton, ON L8P 4Y5

Angela Storey

905-546-2424 ext. 6483

Angela.Storey@Hamilton.ca

April 2016

Ongoing Project

EMS vehicles that required integration with Bluetooth, Garmin devices for in-cab communication with Central Ambulance Control Centre and Ministry of Health and Long-Term Care reporting system as well as PTO reporting for lights, sirens.

Roads & Maintenance vehicles - design and creation of a Public access website, a mobile app for contractor specific application, integration to spreader controllers, and PTO status for winter snow plows.

Simple track and trace for Parks and Recreation, Animal Services, Buildings, By-laws, Cemeteries, Forestry, Hamilton Water, Horticulture - 750 Units to date.

\$5 Million

Reference (4)

Hydro One Networks Inc.

6975 Kenderry Gate | Mississauga, Ontario L5T 2Y1

Frank Currie

Manager - Fleet Services

(905) 696-7190 x 3315

frank.currie@hydroone.com

October 2013

December 2016

SkyHawk Telematics provided Hydro One with a complete telematics solution that facilitated fleet monitoring for multiple lines of business including Construction Services, Forestry, Provincial Lines, Fleet and Station Services. Over 5000 vehicles

were installed with a dual-mode cellular/satellite solution to equip its fleet comprised of the boom truck, off-road and light-duty vehicles. The hardware installation and testing was a joint effort between the Hydro One mechanics and SkyHawk technicians, taking approximately 22 months to complete.
\$20 Million

Reference (5)

City of Davenport Iowa

226 West 4th Street, Davenport, IA52801

Art Bartleson

Director of Public Works Street Maintenance Supervisor

(563) 327-5114

abartleson@ci.davenport.ia.us

December 2015

November 2016

Installed SkyHawk 4G GPS/AVL system in late 2015 to replace an existing 2G system from another vendor. Davenport monitors their salt spreaders equipped with FA5100 and FA6100 controllers, graders, and supervisor vehicles. They use the live "Route Service" mapping overlay to monitor winter operations. SkyHawk has developed a printable route completion report for drivers coming on shift; testing at Davenport and other customers is helping developers maintain a timeline for an early fall release. City snow operations staff use SkyHawk to manage material usage, report costs and improve efficiency. Waste Department on boarded 2020 with 31 garbage trucks.

\$82,000.00

d. Overall interoperability of turnkey system for government use

SkyHawk's strength is in its ability to meet the needs of a very diverse fleet such as government requirements Our current client portfolio includes large cities, municipalities, utility companies, construction companies as well as simple delivery vehicles.

SkyHawk Telematics is device agnostic. We pick the best hardware manufacturers from around the globe to address each vehicle type requirements, from simple track-and-trace, to complex spreader integrations, to vehicles with multiple IO requirements.

Each piece of hardware is selected to fit perfectly each vehicle's specific requirement and not one piece of hardware is made to fit all. Partnering with multiple hardware vendors also means that we are able to offer our clients the most current and up-to-date hardware, ensuring that we **future proof** your solution by not only meeting their requirements for today but being flexible to anticipate and meet future requirements.

The modems we offer have a robust set of features with reliable track records, including standard store- and-forward capabilities for when the vehicle is out of cellular coverage, as well as the ability to receive and perform over-the-air (OTA) configuration or firmware updates in the field.

This eliminates the need to physically visit the vehicle for support and maintenance. SkyHawk's most widely used modems range from simple track and trace to the most complex of applications used for optimal winter maintenance tracking.

e. Accessories available for turnkey offering

In addition to SkyHawk's flagship product ConnectAnywhere, the following are available for easy add-on functionality.

Route Optimization

SkyHawk partners with Quetica to offer a Route Optimization solution for our clients. Route optimization is a mathematical analytics approach that uses sophisticated optimization algorithms and big data technologies to find the best solutions. Examples of optimization applications in business include determining best routes, schedules, capacity, and pricing to maximize return on investment from materials, labor and equipment.

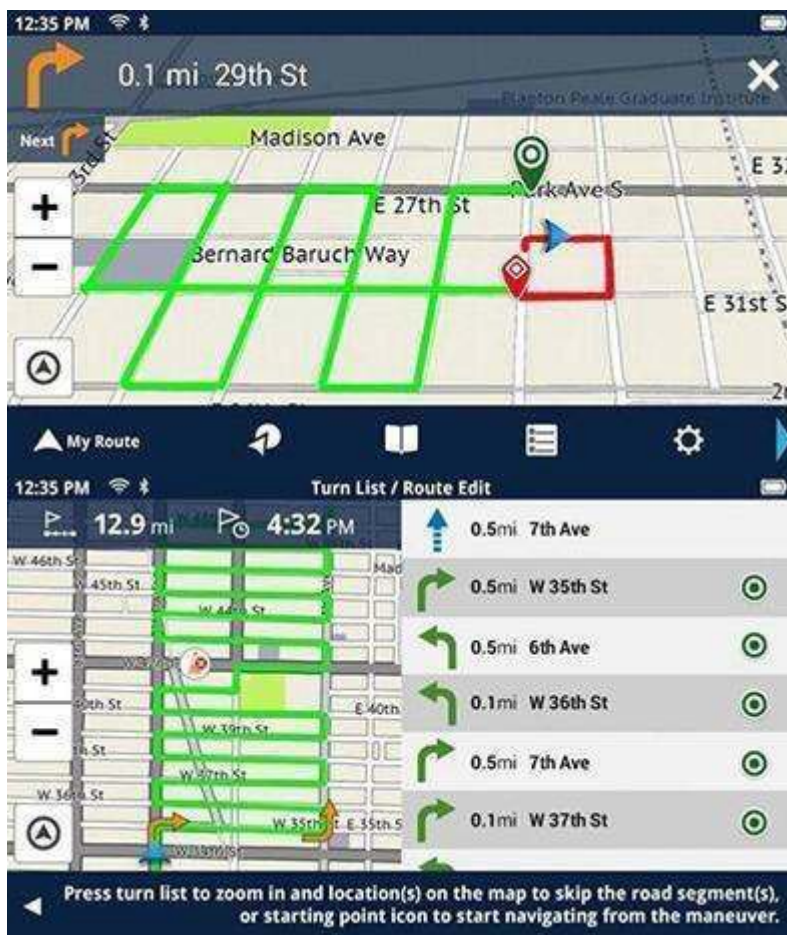
In-cab Turn-by-Turn Navigation and Routing

In cab, turn-by-turn navigation is offered through our partner Magellan. Utilizing the Magellan RouteComplete System. RouteComplete allows administrators to easily pre-schedule, adjust and update routes over the air from the back-office. All routes are loaded on the device allowing route change to be sent to the drivers. RouteComplete was designed for route planning in complex, highly dense urban canyon environments where accuracy can be a challenge. RouteComplete includes Return-to-Route advanced features such as Locked-on-Route, Deviated-Point-Navigation, Event-Driven Re-Routing, High Accuracy GPS, Real-Time Route Completion Monitoring and Real-time Route Management.

The driver can use the tablet touch screen to identify areas where they cannot proceed and identify the issue (temporary road closures, double parked cars, construction etc.). The tablet navigation software will then navigate the driver to the closest area where they can resume the route. The administrative portal will display these areas on the map display for all routes.

The in-cab tablet provided is the Magellan Kiron Tablet, specifically designed for use inside a Winter Operations vehicle. The tablet is a touch screen, ruggedized, with voice commands that can easily be heard in loud environments. The tablet comes in two versions, an LTE version that utilizes its own sim card for data transmission, and the Wi-Fi version for connecting to a SkyHawk modem and utilizing the modem hotspot for data transmission.

The tablet can be unlocked for use with other applications and email; however, it is an Android based tablet, and The Route Complete System is currently only available on Android based devices.



SkyTrak Mobile App – Driver & Vehicle Tracking

SkyTrak is a mobile app that provides a simple and cost-effective telematics solution for tracking for temporary workers, leased vehicles and contractor fleets. SkyTrak may also be used in a standalone fashion as the primary means to monitor a customer's fleet.

The SkyTrak app is available free of charge from either the Apple App Store or Google Play.

The SkyTrak app provides rapid, almost immediate deployment to provide a set of features in ConnectAnywhere. SkyTrak relies on a smartphone's existing cellular or Wi-Fi connection provides a zero-acquisition cost solution to basic fleet tracking.

There is a monthly fee for accessing the data on the ConnectAnywhere site. SkyTrak will not function unless a valid user account and list of vehicles is created for the app user to sign in and use.



Designed for ease of use and simplicity for the operator, the app only requires the driver to identify themselves (through login) and select the vehicle they are driving. Subsequently, start and stop buttons enable and disable tracking respectively.

The app currently provides the following functionality:

- Live GPS tracking
- Driver ID
- Route servicing
- Reporting
- Contractor payment reconciliation
- Contractor sub-account access

SkyHawk plans to further develop the app by integrating additional onboard sensors. Chief among these are retrieval of engine diagnostics and other information through the use of inexpensive and readily available off the shelf OBD2 Bluetooth adapters, and specialized salt controller data and digital inputs.

PlowTracker Public Website

The SkyHawk Telematics PlowTracker public website is designed with the following features:

Display Client's winter vehicles (equipped with SkyHawk Telematics AVL) current position on Google maps for the public viewing. This feature does not display routes. Clients can decide which vehicles are shown on the public site by selecting them via the "Public Site" menu option.

PlowTracker shows Municipal and contractor plows working together to clear roads. On other days, or if a significant snow event is forecasted, Plow Tracker may show Municipal plows doing preventative winter road maintenance like using salt and brine to keep the roads clear of ice.

System provides a configurable delay for vehicle position (i.e. 5 min delay). This feature is designed to add some protection for the Operators as displaying live data may allow the public to intercept trucks and interfere with standard plowing operations. The delay is configurable to any number of minutes via the "Public Site" menu option. The timed delay can be disabled by setting the delay status to 0.

There is a minimum speed configuration option. If vehicles are travelling below a specified threshold the selected vehicles will be hidden to the public. This can also be disabled by setting the minimum speed to 0.

The public can select how much previous data they want to view either 2, 4, 12 and 24-hour periods. The screenshot below shows a bread crumb trail of routes completed in the past 4 hours as per the selected time frame.

Public Website

The public will have viewing rights to the vehicle icon only; vehicle id, driver ID, or speed is not displayed.

Clients have the ability to overlay with specific layers including MTO camera system. The site can be configured with a geographical "boundary". Any messages, vehicle icons that occur outside this boundary will not be shown. The user has zoom in/out functionality on the Google Map.

Driver ID – Key Fob

Each driver gets a unique key fob, required for each journey, a key reader to ID drivers is installed on the vehicle's dash along with our GPS tracking unit. When the vehicle is turned on, the driver presents the key fob into the key reader.



I-Button Reader Assembly (Includes Reader, key fob, jBuzzer, 4-wire)

Enterprise Level and Third-Party Integrations

ConnectAnywhere uses a REST API to easily integrate into third-part applications. The REST API provides simple read-only access to the most important data items in the ConnectAnywhere database: assets (both static attributes and current dynamic state) and messages (data points or transactions). It is an HTTP-based interface implemented using REST (Representational State Transfer) principles, intended to be used by application developers who wish to transfer asset and message data to third-party systems or data management tools. By using JSON and HTTP/HTTPS the API can easily be accessed by an application using any of a variety of languages.

f. Thoroughness of the vetting process used to select partners

SkyHawk owns and has designed and built the cloud-based telematics software solution ConnectAnywhere, however a technical partner ecosystem is utilized for various aspects of our solution including the cloud-hosting, database managed services, mapping interface, in-vehicle data collection and communications hardware as well as interfaces to other third-party software applications as may be required by the client.

SkyHawk's partnerships, which support our main ConnectAnywhere cloud-based application, mainly consist of large, leading enterprise-based organizations such as Google, MongoDB and Amazon (AWS). The other major component of our technical partner ecosystem includes the companies that provide physical hardware included telematics modems, cabling and sensors which collect and transmit data from the vehicles. To ensure we are not exposed to any major supply chain issues (including those caused by COVID-19) SkyHawk holds a significant inventory of most all its major components for rapid and easy distribution to our clients.

An example of our success with partnering is for the City of Pittsburgh. As part of a public bid award, SkyHawk partnered with Quetica LLC, and Magellan Solutions provided the City of Pittsburgh with a complete Telematics Solution, Route Optimization, and Route Navigation system. 138 winter vehicles were installed in Phase 1 of the project during Q4 2018, with a mix of approx. 350 heavy and light-duty installation during Phase 2 of the project in Q4 2019.

As for the vetting of these partnerships, anything development related is trialed, tested, and proven for our needs wherever possible by our development team before releasing to our clients. The same is true for our hardware solutions. We have a hardware specific department that ensures the solution we recommend works, especially for each client's needs and specific environmental conditions.

g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

SkyHawk will provide installation technician(s) who shall provide installation services, installation training and hardware troubleshooting services to the client during the hardware installation rollout. The SkyHawk appointed PM will collaborate with the client on installation locations and logistics at the client preferred locations.

SkyHawk will provide the sub-contractor with a suitable quantity of spare parts for service calls so they can complete most minor repairs on the first visit.

Sample AVL Validation Checklist

This form is to be populated by the installer and a scanned copy is to be submitted to SkyHawk for record and reference



AVL Validation Checklist

GENERAL INFORMATION					
Client Name	City of Mississauga	Vehicle Number			
Vehicle Make/Model/Year					
Odometer Reading	☐ Miles ☐ KM	Engine Hours			
ECM Type	☐ OBD2 ☐ J1939 Type 1 ☐ J1939 Type 2 (Green Connector) Other:				
Modem Type / Serial #					
Spreader Make / Model					
Driver ID Enabled	☐ Yes ☐ No	WiFi Enabled	☐ Yes ☐ No		
CONNECTANYWHERE - BASIC TEST RESULT CHECKLIST					
Item	Test Procedure (indicate ☒ for Pass, ☐ for Fail & record notes on failure)		✓		
GPS Position	Search for the vehicle using the ConnectAnywhere Assn. List , verify location on map is correct and it is showing correct date and time.				
Ignition On/Off messages	Cycle engine - Review History Report for Ignition On and Off messages				
Odometer/Eng Hrs reading	Verify the History Report displays correct odometer and engine hour readings				
ECM Data (if applicable)	Export History Report into Excel, verify VIN and other engine data is displayed				
Driver ID (if applicable)	Turn vehicle Ignition On , scan the Driver ID Fob/card to authenticate on the system, verify the Driver ID is displayed in the History Report & mouse over				
Spreader (if applicable)	Set a spread rate on the controller, verify in History Report the set rate selected and actual rate is displayed. Ensure accumulated totals for weight and distance increase.				
Idle Time	Ensure vehicle has been idling for greater than 5 minutes, turn ignition off and verify the History Report displays correct idle time				
INPUT TEST RESULT CHECKLIST					
Input Test Procedure: Change the status of the Input from Up/Down, On/Off or In/Out and verify the correct status is displayed by refreshing the History Report. ☒ = Pass ☐ = Fail					
Input	✓	Input	✓	Input	✓
Front Plow		Right Boom		Other (list):	
Wing Plow		Left Boom		Other (list):	
Belly Plow		Centre Boom		Other (list):	
Beacon 1 (indicate color)		TO		Other (list):	
Beacon 2 (indicate color)		Boom		Other (list):	
TESTER SIGN OFF					
Notes: Record any failures or anomalies with the vehicle and call the SkyHawk Support Desk for assistance troubleshooting.					
Spreader Controller Calibration:					
Tested By					
Date					

NOTE: The system will not function correctly if tested inside a building. Ensure to test when vehicle is parked with clear view of the sky, away from buildings or the tree line.

Please scan and email the completed form to your SkyHawk Telematics deployment representative.

For assistance with testing or troubleshooting call the SkyHawk Telematics Support Desk at 1-844-424-7759, Option 2.

V1.0 - 2019-11-27

Troubleshooting and Configuration Changes

The SkyHawk Support Desk will assist the Customer with troubleshooting malfunctioning hardware devices. If the device can't be fixed through Over the Air (OTA) configuration changes, manual reprogramming or additional diagnostic measures, the SkyHawk Support Desk will recommend either returning the device to SkyHawk for repair or dispatch a field technician for a service call.

The Customer shall contact SkyHawk Support Desk when making the following configuration changes:

- Baseline odometer or engine hour value
- ECM type
- Change to vehicle voltage of AVL modem device
- Change to installation method of AVL modem device (3-wire, hardware ignition only, or ECM power)

Installation, Removal or Repair of Hardware

The Customer shall contact the SkyHawk Project Manager or SkyHawk Support Desk to schedule a service call if a unit is to be removed, installed, or needs repair. SkyHawk will dispatch a trained, qualified service technician to the Customer site. SkyHawk technicians are equipped with a small stock of commonly used spare parts so they may complete a repair during the same service call as the initial troubleshooting. Equipping our Service Technician with spare parts results in both time and cost savings for the Customer.

Ordering Hardware

The Customer shall contact their SkyHawk Account Manager to place an order for hardware. A quote will be provided for the Customer's review and approval. A P.O. is required from the Customer to authorize the purchase.

Winter Hardware Validation Testing

SkyHawk will assist the Customer with training and a test plan to efficiently conduct its own Winter Hardware Validation Test to ensure the winter equipment is re-installed correctly and operating as expected. This test is encouraged every fall before the start of the winter season. SkyHawk can also provide trained technicians to conduct the test for an additional fee.

Return Material Authorization (RMA)

The Customer shall contact the SkyHawk Support Desk to obtain authorization before returning any defective or un-used hardware. The SkyHawk Support Desk will respond in writing with the RMA number, return address and instructions for preparing the courier documents.

Discontinued Hardware

When a hardware device is to be discontinued, the SkyHawk Account Manager will notify the Customer in writing of the discontinued product and will provide as much advance notice as possible. A suitable replacement will be recommended by the Account Manager with an accompanying price quote. The SkyHawk Support Desk will provide an installation guide and assistance to install the new device for a demo period or can arrange for a service call to have the new device installed by the SkyHawk approved installation sub-contractor.

Communication

Regularly Scheduled Software Release and Maintenance Update

The SkyHawk Support Desk will notify key personnel of the Customer via email five (5) business days in advance of an upcoming Software Release and Maintenance Update. The first notice will include the date/time and approximate duration of the maintenance window. A reminder email is sent the day of the update and this notice will include the release notes. Once the update is complete, the release notes can also be found on ConnectAnywhere under the Help menu.

Service Interruption or Unplanned Outage

The SkyHawk Support Desk will notify key personnel of the Customer via email as soon as possible when any service interruption or unplanned outage of the software is detected. The Support Desk will continue to provide regular updates via email until the issue is resolved.

Annual Meeting

At minimum, the Customer and SkyHawk will meet twice annually; in October to prepare for the upcoming winter season and then again in April to prepare for summer operations. Items on the agenda will include:

- Review any major software updates to the system
- Determine if any additional system training is required
- New hardware requirements (spare parts and/or new kits)
- Requirements for Installation Service (service calls and/or new installations)
- Vehicles that require suspended service (to be discussed in the spring meeting)
- Review of any outstanding Support Tickets/Issue Log

SkyHawk Support Personnel

SkyHawk Support Team

SkyHawk's Technical Support Team works closely with the Project Management Team and Installation Technicians to offer deployment and post-sales support to our Customer base. Customers can reach the Support Desk via a toll-free support line 1-844-424-7759 ext. 2 or by sending an email to support@skyhawk.co. All issues that are emailed to support are automatically logged as a ticket in the JIRA issue-management system. Level 1 Support is the initial point of contact provided by SkyHawk. Any issues that can't be resolved by Level 1 are forwarded to the Level 2 Development Manager to assign the appropriate resource for resolution.

Level 1 Support

SkyHawk's experienced frontline Level 1 Support Team product specialists handle the lion's share of the trouble tickets on a day-to-day basis. Level 1 can assist with website and report issues, system administration, hardware configuration, installation support and hardware diagnostics/troubleshooting. All issues reported to Level 1 are logged in the Jira issue-management system and triaged based on severity outlined in our Service Level Agreements. Support resources will make every effort to resolve the issue as quickly as possible. Issues that can't be resolved by Level 1 Support are escalated to Level 2 Support.

Level 2 Support

Level 2 support is comprised of a team of highly skilled software developers and hardware engineers located in SkyHawk's head office in St. John's, NL. Level 2 support will evaluate the issue and advise the SkyHawk Project Manager/Account Manager of the expected resolve date, who will communicate back to the Customer's Project Manager and/or the person who raised the ticket. Issues that are considered low risk may be implemented into the production environment as "Hot Fixes", while fixes that require more development effort and testing are scheduled for implementation into a regularly scheduled maintenance release, which typically takes place once per month.

SkyHawk Support Team			
Team Member	Project Position	Phone	Email
Support Team – Level 1	Product Support Specialists	1-844-424-7759 x2	support@skyhawk.co
Krista Schmidt	Director of Operations	289-270-0899	Krista.schmidt@skyhawk.co
Mark Callahan	Subject Matter Expert – Software – Level 2	709-737-2583 x27	mark.callahan@skyhawk.co
Derrick Dunne	Subject Matter Expert – Hardware – Level 2	709-737-2583 x32	derrick@skyhawk.co
Sean Hogan	Subject Matter Expert – System Architect - Level 2	709-737-2583 x31	sean@skyhawk.co

The SkyHawk Support Team is available 8:30 am – 5:00 pm, Monday through Friday for email and Telephone support. Emails are not monitored outside of business hours however Telephone support is available 24/7/365 for Critical Issues classified as Priority 1 or Severity 1.

After Hours Response for Critical Issues

Any issues called into the Technical Support Line outside of SkyHawk business hours are automatically forwarded to Telelink call centre that operates 24/7/365. Any issues that can't be resolved by Telelink and are determined to be critical in nature are escalated to the appropriate personnel via the emergency call out procedure. Examples of critical issues are website down/users cannot log in, or the system is up but the vehicles are not updating with live data. SkyHawk will take appropriate actions and pull together the resources necessary to resolve critical issues as quickly as possible. Any non-critical issues are deferred to the SkyHawk level 1 support team to address the next business day.

Account Manager

After the project implementation is complete, the Account Manager will take on the role of the Customer's main point of contact for any issues besides regular ongoing support. The Account Manager is responsible for ensuring the Customer is kept up to date on the software development roadmap and new hardware technologies. The Account Manager is also responsible for providing quotes when reordering hardware or sourcing new products, establishing regular meeting intervals and coordinating training as required.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

a. Pre-installation coordination

At SkyHawk, careful planning and collaboration with the client will ensure a successful "Go Live". As part of the planning process, we establish clear benchmarks by which a project team can measure progress. These benchmarks make it clear where a project stands and allows adjustments to be made in the event changes are required.

The Go-Live Assessment and Plan is intended to aid the project and stakeholders in planning for the AVL installation, testing and roll-out. It can be used to plan the go-live event and to identify any issues that need to be addressed beforehand. The checklist will help eliminate some of the "unknowns" that often occur on the first day of system implementation.

Go-Live planning includes, but not limited to:

- Set the Go-Live date with the client
- Use the Go-Live date to plan all aspects of 50 Proof of Concept vehicles, UAT and roll-out completion and to allow for contingencies.
- Determine the rollout strategy; installation of 50 Proof of Concept vehicles, priority winter vehicles and all remaining vehicles to be outfitted with the AVL equipment.
- Communications to key individuals such as, project team members, stakeholders, yard superintendents, of go-live date when it appears certain and request their support during the installation
- Review goals and objectives with key stakeholders and reaffirm. Make any necessary changes as required in order to accomplish the client's goals and objectives.

The following is a sample Go-Live Assessment and Plan for the client's AVL project:

Task	Status	Comments
Contract Award	Completed	Communication
Project Managers Appointed	Completed	Communication

Kick-Off	Scheduled	
Requirements Capture	In Progress	
Delivered Project Management Documentation	In Progress / On-Going	
Hardware Delivered	In Progress	
Delivery of ConnectAnywhere Training for End Users	In Progress	
Delivery of AVL Hardware Installation to client Technicians	In Progress	
Proof of Concept 50 Vehicles - UAT Pass	In Progress	General Comm. of UAT Pass
Systems Validation & User Acceptance Test Ends	In Progress	
Prioritized Winter Vehicles - UAT Pass	In Progress	General Comm. of UAT Pass
Systems Validation & User Acceptance Test Ends	In Progress	
Remaining AVL Equipment Installed	Not Started	
Systems Validation & User Acceptance Test Ends	In Progress	
Transition to Operational Support	Not Started	
Meeting - ~1 Week to Go-Live	Not Started	Communication of Status
Meeting - ~3 Days to Go-Live	Not Started	Communication of Status
Meeting - Go-Live Day	Not Started	General Comm. of Status Go-Live
Post Go-Live Stabilization Period	Not Started	
Lessons Learned Captured	Not Started	
Close	Not Started	

b. Project coordination

SkyHawk's Project Team utilizes the Project Management Institutes (PMI) project methodology phased approach that is broken down into five (5) process groups: Initiate, Plan, Execute, Monitor and Close. In each process area we have identified key documents and tools to serve as inputs which result in deliverables for each phase.

SkyHawk's project team will spend a considerable amount of effort on detailed requirements gathering to ensure a complete understanding of the client's needs and will compile a comprehensive Project Plan which we feel is critical to the project success. The Project Plan will be updated regularly as the project progresses, and will establish project roles and responsibilities, detailed schedule of tasks, Quality Plan, risks, and Change Control. Additionally, SkyHawk's project team will work with the client's project team in preparing a full updated project schedule, including the client's installation schedule. Bi-weekly status meetings will be held to review the project schedule and to review any open issues in SkyHawk's JIRA ticketing system.

Project Communication: Project Communication will be established in the form of a regularly scheduled project meetings with status reports issued weekly. The status report will contain at a minimum the following information:

- Dashboard view on the progress of installations, tracking completed installs to planned

- Task/Action Item List from previous meetings
- Defect/ Issue Log generated from the Jira Ticketing System

In addition, SkyHawk will collaborate with the client on preparing awareness communications for ConnectAnywhere training, hardware installation training, etc. as appropriate.

Communication Plan: The Project Communication plan will be created in partnership with SkyHawk and the client's Project Managers to outline how the AVL project team will be communicated during the project.

The Communication Plan shall be completed early enough in the project to be included for review at the Project Kick-off Meeting. Communications include but not limited to status, meetings, issues, deliverables access, and design/ document reviews.

Below is a **sample Communication Plan:**

What	Who / Target	Purpose	When / Frequency	Type / Method	Date Complete
Discovery Meeting	All stakeholders	Identify all stakeholders and provide a forum for all project team members to discuss schedule, scope, team, communications, and other items	As many as required at the start of the Project Initiation phase - 60-90 minutes session(s)	Meeting - In person / Virtual	
Project Kick-off Meeting	All stakeholders	Familiarize the project team and stakeholders with the project, review the project charter and receive buy-in from all project participants. Future meeting schedules will be defined and discussed, and meeting minutes will be documented.	At the end of the Project Initiation phase. - 60-90 minutes	Meeting - In person	
Awareness Communication: General information of AVL Project	TBD	Communicate general information to Stakeholders about coming changes	Two months before implementation. Two weeks update about changes. Two days before implementation	Email to appropriate stakeholders using the client's communication process	
Team Status Meeting	Entire Project Team	Review Project Register: Tasks, Schedule, Assignments, RAID Log, Change Requests, Open Tickets	Regularly Scheduled. Weekly/Bi-Weekly (30-60 minutes)	Meeting - In person / Virtual Meeting with standardized agenda and minutes.	

Sponsor Meetings	Sponsor(s) and Project Manager	Update Sponsor(s) on status and discuss critical issues. Seek approval for changes to Project Plan.	Monthly and/or as needed when issues cannot be resolved, or changes need to be made to Project Plan - 30-60 minutes	Meeting.	
Training Awareness Communication to ConnectAnywhere Users	Users of the application	Inform users of the changes to the existing application	Two weeks before implementation. Two days before implementation	Training: TBD Targeted email communication to system users	
Periodic Demos and Targeted Presentations	Specific Groups and/or End Users	To gain input from specific groups and keep end users apprised of features	As needed to demonstrate functionality and receive feedback in a timely manner - 30-60 minutes, as required	Meeting - In person / Virtual Presentation and Discussion	
FAQ	Users of application	Document and communicate Frequently Asked Questions about the application captured from various inputs	As needed.	Email	
Project Closing Meeting	Project Manager, Project team, key stakeholders, and sponsor(s)	Conducting the post project review meeting will allow the project team and the client's project participants stakeholders to gather one last time to ensure that there are no outstanding issues or work. This will also provide a forum to review lessons learned throughout the project.	End of project or end of major phase - 60-90 minutes	Meeting - In person / Virtual Standardized agenda and minutes.	
Other...	TBD by the team.	General communications.	As needed.	TBD	

Reporting Methods: During project implementation, the Status Report will be issued bi-weekly, prior to the Project Team Meeting. The Status Report will contain percentage complete and dashboard views of scope, schedule, cost, and quality. It will be prepared in formats approved by the client's, and will contain at a minimum the following information:

1. Progress Dashboard showing percentage complete from previous meetings.
2. Defect Log generated from the Jira Ticketing System.
3. Project Status as it relates to the Work Plan.
4. Deliverables status.
5. Planned activities for the upcoming two (2) week period.
6. Future activities.
7. Requirements Traceability Matrix (RTM)
8. Report and remedies in case of falling behind Schedule.

- 9. User Acceptance Test Feedback
- 10. Risk/Action/Issues/Decision (RAID) Register

c. Installation and Testing process

All SkyHawk's products are highly tested to ensure optimal quality. A description of the processes is as follows:

Our software development team uses an Agile product development methodology. Agile development is a group of software development methods in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, continuous improvement, and encourages rapid and flexible response to change. Key features of the Agile method include early and frequent releases of new products, in small fully functional units. This promotes early customer engagement and feedback which guides the continued development of a feature into its final form. Sales, project management, and development staff are all key contributors to the process. Clients may also be directly engaged in the process or may be represented by the sales or project management staff.

SkyHawk has established methodology and procedures for Quality Assurance and Control for hardware and software validation through a variety of test methods, checklists, and test plans, change control, and corrective action plans. Everyone is responsible for delivering quality work in their respective area. For a full description of SkyHawk's testing procedure, please refer to Installation Plan.

SkyHawk manages software configuration through Subversion, in combination with a commercial issue-management system called JIRA that records all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration).

SkyHawk employs JIRA to record all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration). The workflows established in JIRA are integrated with the Company's Agile software development process.

We schedule maintenance releases each month, if warranted. New feature releases are incorporated into this schedule as required, with initial deployment on a test system for internal validation. In addition, Priority 1 or Severity 1 defects are addressed in real time with a fix or patch applied to the affected system(s) as soon as they are available and tested. Priority 1 defects are defined as issues which have rendered a system feature inoperable, without a workaround. Severity 1 defects are defined as issues which have not occurred but which, if triggered, would result in an impact like a Priority 1 defect.

SkyHawk Telematics applies a Lean Process philosophy to all aspects of its day to day operations, including software development, which supports increased productivity, competitiveness, and continuous improvement, while empowering our employees to problem-solve and strive for organizational excellence. Our Software Development Group adheres to well-defined processes to ensure that its services are provided in a focused manner. Under this methodology, requirements are clearly defined, progress against goals can be measured, and reliable software is produced.

All defects found during User Acceptance Testing must be reported to SkyHawk Project Manager for entry into the Jira ticketing system. The Project Manager will record the details of the defect under the Issue Type "Bug" and include the following information:

- Date/Time the defect was created
- Who reported the defect?
- Brief Summary of the defect
- Detailed defect Description including steps to reproduce the defect
- Software or hardware component(s) affected
- Any associated documents are added to the Jira ticket as Attachments i.e.: Test Plan, Test Results, screenshot(s) of defect

After the defect information is captured, the ticket will be triaged by the Support Desk, assigned a Severity Level and then the ticket is assigned to the resource(s) best fit to resolve the issue. All defects logged into Jira are exportable into a Defect Log Report in either MS Excel or PDF format.

d. Client Infrastructure and support assessment process

SECURE DESIGN

SITE SELECTION: Prior to choosing a location, AWS performs initial environmental and geographic assessments. Datacenter locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another.

REDUNDANCY: Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY: AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Using Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

CAPACITY PLANNING: AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

BUSINESS CONTINUITY & DISASTER RECOVERY

BUSINESS CONTINUITY PLAN: The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

PANDEMIC RESPONSE: AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

MONITORING & LOGGING

DATA CENTER ACCESS REVIEW: Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in

accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

DATA CENTER ACCESS LOGS: Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

DATA CENTER ACCESS MONITORING: We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV: Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS: Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION: Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require everyone to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

DEVICE MANAGEMENT

ASSET MANAGEMENT: AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

MEDIA DESTRUCTION: Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

OPERATIONAL SUPPORT SYSTEMS

POWER: Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

CLIMATE AND TEMPERATURE: AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION: AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION: In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

EQUIPMENT MAINTENANCE: AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

ENVIRONMENT MANAGEMENT: AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

ONGOING DATA CENTER RISK MANAGEMENT: The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business. This process also takes regional regulatory and environmental risks into consideration.

THIRD-PARTY SECURITY ATTESTATION: Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

- e. End user Acceptance process

SkyHawk Telematics has extensive hardware validation testing and full system user acceptance testing procedures that the project management team conducts during and after installations. SkyHawk will collaborate with the client to perform system testing and validation. The Project Manager will provide standard test plan templates and will assist the client with User Acceptance Testing. Training will be provided to the client's staff on how to properly test and validate software and hardware. The client's staff are encouraged to participate in all areas of system testing as we feel it provides them with a greater understanding of the system and leads to earlier adoption.

The SkyHawk Support team will provide technical support during the testing process. Over-the-air updates and configuration can be sent by the support team, as well as assisting the technicians with onsite programming. The client's personnel shall be present at all installation locations to observe all testing procedures performed. The testing team will be

provided full training documentation, including the ConnectAnywhere™ system user guide, hardware information and troubleshooting guides.

The following is an outline of testing to be performed by the Project Team:

Testing Strategy: SkyHawk will use live real-time data and historical data from the time of vehicle installation to validate the information provided in the system is correct. All testing will be performed on the City's SkyHawk ConnectAnywhere system with SkyHawk helping to facilitate the list of tests established.

Test Procedures: SkyHawk personnel will assist the City through the detailed list of tests established in the Test Procedure document

Demonstration: Through a detailed list of step by step process, SkyHawk will demonstrate to the City the functionality of the different features that were requested. This includes vehicle input status, real-time notification, and data accuracy.

System Validation Testing: This testing is performed by SkyHawk to validate the ConnectAnywhere website is set up per the client's requirements and the website is functioning as expected. This test is typically completed one week prior to installations. All mapping functions and menu items are tested for expected behaviour and to ensure of customer-specific requirements are available on the website. Phase 2 is conducted in the early stages of installation, usually, on the first or second day after some vehicle installations are complete and, real-time data is available for the testing.

This testing will include data accuracy drive tests, real-time alerts, and report data validation.

Hardware Validation Testing: This testing is performed by the Installation Technician on each vehicle in the final stage in the installation process to ensure the hardware is installed correctly and the modem has been updated with the correct configuration. This test includes verification of GPS message data, ignition on/off, idle verification, spreader integration, input status, and power shutdown.

Calculation: Determine the run time calculations, amount of material used, average spread rates and verify the reports represent the calculated values.

User Acceptance Testing (UAT): SkyHawk will work collaboratively with the clients to perform User Acceptance Testing on the selected vehicles. First, the selected vehicle(s) must complete the prerequisite Hardware Validation Testing. Next, the basic system functionality will be verified on the website in addition to a drive-test to verify real-time alerts and validate data collected in the reports such as spread rate of salt, liquid rates, the total amount disbursed, geofenced area and plow up/down. The steps to perform this test will be recorded in the approved UAT test plan. The Client will record comments from the test process and indicate Pass or Fail. Any items with a fail will be recorded in the Jira ticketing system to track issue resolution.

Analysis: Verification of vehicle test runs where actuals are recorded and compared to the output on the system reports.

Test Management: System Validation, Hardware validation, Calibration testing, IAT and Commissioning Test will be conducted by the City and SkyHawk before testing is being executed by the City staff with assistance and guidance from the SkyHawk project team. Using the SkyHawk Test Procedures, the PM will record those features that were successful and those that require additional testing. For all items that require additional testing, details notes will be taken and reviewed by NHDOT. These notes will also allow SkyHawk and the City to determine which subsequent tests need to be performed to ensure all features are functioning properly.

f. Approach to maintenance and support

All SkyHawk's products are highly tested to ensure optimal quality. A description of the processes is as follows:

Our software development team uses an Agile product development methodology. Agile development is a group of software development methods in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, continuous improvement, and encourages rapid and flexible response to change. Key features of the Agile method include early and frequent releases of new products, in small fully functional units. This promotes early customer engagement and feedback which guides the continued development of a feature into its final form. Sales, project management, and development staff are all key contributors to the process. Clients may also be directly engaged in the process or be represented by the sales or project management staff.

SkyHawk has established methodology and procedures for Quality Assurance and Control for hardware and software validation through a variety of test methods, checklists, and test plans, change control and corrective action plans. Everyone is responsible for delivering quality work in their respective area. For a full description of SkyHawk's testing procedure, please refer to the Installation Plan.

SkyHawk manages software configuration through Subversion, in combination with a commercial issue-management system called JIRA that records all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration).

SkyHawk employs JIRA to record all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration). The workflows established in JIRA are integrated with the Company's Agile software development process.

We schedule maintenance releases each month if warranted. New feature releases are incorporated into this schedule as required, with initial deployment on a test system for internal validation. In addition, Priority 1 or Severity 1 defects are addressed in real-time with a fix or patch applied to the affected system(s) as soon as they are available and tested. Priority 1 defects are defined as issues that have rendered a system feature inoperable, without a workaround. Severity 1 defects are defined as issues that have not occurred but which, if triggered, would result in an impact similar to a Priority 1 defect.

SkyHawk Telematics applies a Lean Process philosophy to all aspects of its day to day operations, including software development, which supports increased productivity, competitiveness, and continuous improvement, while empowering our employees to problem-solve and strive for organizational excellence. Our Software Development Group adheres to well-defined processes to ensure that its services are provided in a focused manner. Under this methodology, requirements are clearly defined, progress against goals can be measured, and reliable software is produced.

All defects found during User Acceptance Testing must be reported to SkyHawk Project Manager for entry into the Jira ticketing system. The Project Manager will record the details of the defect under the Issue Type "Bug" and include the following information:

- Date/Time the defect was created
- Who reported the defect?
- Brief Summary of the defect
- Detailed defect Description including steps to reproduce the defect

Software or hardware component(s) affected

Any associated documents are added to the Jira ticket as Attachments i.e.: Test Plan, Test Results, screenshot(s) of defect

After the defect information is captured, the ticket will be triaged by the Support Desk, assigned a Severity Level and then the ticket is assigned to the resource(s) best fit to resolve the issue. All defects logged into Jira are exportable into a Defect Log Report in either MS Excel or PDF format.

(b) a description of the methods available for contacting support, days/hours (location time) that support is provided, and your after-hours support. Note: City of Burlington office hours are between 8:30am - 4:30pm local time; maintenance staff typically start at 7:00 am; and asset maintenance can occur 7/24/365.

(c) a description of your process for communicating, prioritizing, and addressing application and infrastructure problems of varying severity levels. The description should include, for different severity levels, how and how frequently the City will be updated and what information will be provided.

(g) a description of the problem tracking data that is collected, maintained and available to the City either online or upon request (e.g. date/time ticket open/closed, problem type, fix, reoccurrence tracking) and for how long.

SkyHawk Support Services

SkyHawk Support Team: SkyHawk's Technical Support Team works closely with the Project Management Team and Installation Technicians to offer deployment and post-sales support to our Customer base. Customers can reach the Support Desk via a toll-free support line 1-844-424-7759 ext. 2 or by sending an email to support@skyhawk.co. All issues that are emailed to support are automatically logged as a ticket in the JIRA issue management system. Level 1 Support is the initial point of contact provided by SkyHawk. Any issues that cannot be resolved by Level 1 are forwarded to the Level 2 Development Manager to assign the appropriate resource for resolution.

Level 1 Support: SkyHawk's experienced frontline Level 1 Support Team product specialists handle frontline trouble tickets on a day-to-day basis. Level 1 can assist with website and report issues, system administration, hardware configuration, installation support and hardware diagnostics/troubleshooting. All issues reported to Level 1 are logged in the Jira issue-management system and triaged based on severity outlined in our Service Level Agreements. Support resources will make every effort to resolve the issue as quickly as possible. Issues that cannot be resolved by Level 1 Support are escalated to Level 2 Support.

Level 2 Support: Level 2 support is comprised of a team of highly skilled software developers and hardware engineers located in SkyHawk's head office in St. John's, NL. Level 2 support will evaluate the issue and advise the SkyHawk Project Manager/Account Manager of the expected resolve date, who will communicate back to the Customer's Project Manager and/or the person who raised the ticket. Issues that are considered low risk may be implemented into the production environment as "Hot Fixes", while fixes that require more development effort and testing are scheduled for implementation into a regularly scheduled maintenance release, which typically takes place once per month.

The SkyHawk Support Team is available 8:30 am – 5:00 pm, Monday through Friday for email and telephone support. Emails are not monitored outside of business hours however Telephone support is available 24/7/365 for Critical Issues classified as Priority 1 or Severity 1.

After Hours Response for Critical Issues: Any issues called into the Technical Support toll-free line (1-844-424-7759 ext. 2) outside of SkyHawk business hours are automatically forwarded to Telelink call centre that operates 24/7/365. Any issues that cannot be resolved by Telelink and are determined to be critical in nature are escalated to the appropriate personnel via the emergency call out procedure. Examples of critical issues are website down/users cannot log in, or the system is up but the vehicles are not updating with live data. SkyHawk will take appropriate actions and pull together the resources necessary to resolve critical issues as quickly as possible. Any non-critical issues are deferred to the SkyHawk level 1 support team to address the next business day.

SkyHawk employs JIRA to record all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration). The workflows established in JIRA are integrated with the Company's Agile software development process.

(d) a description of severity levels (including who determines the severity levels and the process to deal with disagreements), response times, and expected resolution times for each severity level, post-incident reviews and feedback surveys, and escalation processes for emergency technical support. The description should include the hours during which the Proponent will work to resolve issues (by severity level if the hours vary according to severity level).

SkyHawk has three levels of technical support to resolve issues reported by its clients. Level 1 Support is the initial point of contact provided by the SkyHawk Support Team. Any Issues that can't be resolved by Level 1 are forwarded to the Technical Operations Manager to assign a Level 2 resource for resolution. Our frontline Support Desk technicians handle the lion's share of our trouble tickets on a day-to-day basis. Escalation to Level 3 status will involve our software/hardware engineers or field technicians. For problems that require escalation due to urgent nature or unsatisfactory response, the issue can be assigned to our project and company management.

The Help Desk is available 24 hours each day, 365 days per year for reporting of issues and resolution of simple requests: North America: Toll-free number 1-844-424-7SKY (1-844-424-7759) extension #2 or at support@skyhawk.co

Minor Issue - SkyHawk shall respond within 1 business day - At the discretion of SkyHawk, will provide a Workaround and/or Error Correction in the next Version, Upgrade, or Update.

Serious - SkyHawk shall respond the same business day, or if outside SkyHawk business hours, the next business day. - SkyHawk shall provide a Patch within 5 business days following response if possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.

Critical - SkyHawk shall respond the same business day, or if outside SkyHawk business hours, will attempt to respond ASAP, but in all cases within 1 hour the next business day. - SkyHawk shall provide a Patch as soon as possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.

(e) a description of the process by which requests for support can be escalated.

(f) a description of troubleshooting and error tracking methods (e.g. WebEx, Skype for Business, GoToMeeting, remote desktop, system monitoring).

SkyHawk has three levels of technical support to resolve issues reported by its clients. Level 1 Support is the initial point of contact provided by the SkyHawk Support Team. Any issues that cannot be resolved by Level 1 are forwarded to the Technical Operations Manager to assign a Level 2 resource for resolution. Our frontline Support Desk technicians handle the lion's share of our trouble tickets on a day-to-day basis. Escalation to Level 3 status will involve our software/hardware engineers or field technicians. For problems that require escalation due to urgent nature or unsatisfactory response, the issue can be assigned to our project and company management.

A client may request a report of their open/closed issues at any time from our support team.

In addition to reporting issues through the Support Desk, the assigned Project Manager or Account Manager, the Customer may follow this escalation path noted below if a reported problem is not resolved within the expected timeframes or not resolved to their satisfaction:

	Name	Title	Phone	Email
1	Krista Schmidt	Director, Operations	289-270-0899	Krista.schmidt@skyhawk.co
2	Mark Gillingham	Vice President	709-737-2583 x34	mark.gillingham@skyhawk.co
3	Paul Anderson	President	709-737-2583 x24	paul.anderson@skyhawk.co

(h) a description of the warranty for implementation and configuration services, any limitations on the warranty and any limitations on the remedies. The desired warranty is in four parts, one for each phase, the warranty for each phase being for a year triggered by the completion of the phase. Each warranty is for the services provided in the phase.

(j) a description of your Service Level Agreement for cloud solutions including the methodology for granting service level credits and the amount of risk individually and in the aggregate.

Equipment warranty and all service warranty information for the proposed solution.

We warrant that SkyHawk Telematics-Branded Products and all other products and services rented, sold or resold will be free from defects in materials and workmanship for a period of one (1) year from the date of delivery with respect to hardware and will materially conform to their published specifications for a period of one (1) year with respect to software and software-based services.

A sample contract including SkyHawk's End User License Agreement and Warranty policies is attached. SkyHawk offers an Extended Warranty, the cost is 10% of equipment cost per year of the extended warranty period.

- Extended warranty period must be accepted and agreed upon before the end of the manufacturer's warranty.
- Payment for the extended warranty term is due annually based on the client agreeing to the warranty renewal.
- Shipping fees to the SkyHawk office in Oakville, ON are the responsibility of the client. SkyHawk will cover the return shipping fees.
- Costs to remove and re-install equipment covered by warranty are not included in the warranty fee.

(i) if software customization impacts support services how it does so.

The Service Level Agreement for time to resolve issues applies to the production environment only. Issues found when testing customized software will be resolved using best efforts to keep the project schedule, but standard Service Level Agreements do not apply.

(k) a description of any incidents or events that are not included as part of support and any limitations of the Proponent's performance of support including any software currency requirements; and

(l) a description of the anticipated requirements for City staff to support the application and infrastructure (the infrastructure indicated in response to submission requirement 3) directly and what roles are required, and any assistance required from the City in order for you to provide your support services. Include in the description the number (and/or fractions) and types or category of full-time City staff anticipated to be required for this support.

After the project implementation is complete, it is recommended the City to appoint an AVL Coordinator to liaise with the SkyHawk Account Manager. A key responsibility of the AVL coordinator is approve changes in the system such as authorize a new user access or decide who shall have access to a new report offering. A monthly meeting is recommended to review any open issues, be kept abreast of any upcoming changes to the SkyHawk system and determine ongoing needs for training or new equipment installations.

For SkyHawk to support service calls, we must be provided a contact who can arrange for the vehicle to be made available during the service call. Depending on the vehicle type, a vehicle Operator may be required to assist the installation technician with the vehicle testing i.e.: operate the snowplow.

g. Initial and Ongoing Training provided

Training will be provided based on the client's end-user requirements workshop, the personnel's job responsibilities, their interaction with ConnectAnywhere and the various system components. SkyHawk has a comprehensive training team that will provide on-site and / or webinar training as per requirements of the client and will provide full product training for the full group of administrator users. Additionally, SkyHawk will provide web-based remote training on a quarterly basis to all system users to familiarize them with the usage and functionality of the ConnectAnywhere monitoring website. These sessions are intended to reinforce initial training.

SkyHawk will provide the comprehensive set of training materials in both digital and hard copy for all aspects of the ConnectAnywhere system. In-person and/or Webinar training delivery formats are available to the identified end-users of the client.

The training covers all aspects of the system, including:

- ConnectAnywhere Software for Basic End Users
- ConnectAnywhere Software for System Administrators
- Equipment Installation, Diagnostics, Service & Repair

ConnectAnywhere High Level Topics for Basic End-User Training: A full Software tutorial for the end users of the ConnectAnywhere web-based monitoring solution, including but not limited to:

- Log-in and out of Account
- Mapping interface features, including configuration for polygons
- Reporting capabilities
- Geofence creation
- Asset Status features

ConnectAnywhere High Level Topics for System Administrator End-User Training: A full Software tutorial for the System Administrators of the ConnectAnywhere web-based monitoring solution, including but not limited to:

- Creating assets and hardware records
- User logins/account profiles
- Hardware swap procedure
- Decommissioning vehicle procedure

ConnectAnywhere Re-training and Technical Support: Webinars on new features

- Refresher training as needed
- Assistance provided by Support Team
- Support Contract info/hours

In order to satisfy the client's requirement to train end users; SkyHawk's Training Program will be divided into three (3) modules and delivered at various locations as agreed upon with the client. These modules can be modified and tailored to the client's requirements.

ConnectAnywhere Module(s)

Audience	ConnectAnywhere Module(s)	Estimated Duration*
Basic User Overview	Overview of SkyHawk Telematics and interactive/live demonstration of using various functions of the system, such as but not limited to: • Hardware installed and high-level features • Landing Page and Login • Overview of Menu Tabs and Panes • Map View and User Interface • Vehicle Location • History Report and its data • Geofences • Help, User Guides and Release Notes • Question and Answers	~60 minutes
Reporting Overview	Pre-requisite Training Basic User Training Focused training for end users who will be using the system to run reports, such as but not limited to: • Vehicle Trip Report • Speed Report • Winter Operations Trip • Winter – Material by Time • Spreading Speeding • Utilization Report • Scheduled Reports • Help, User Guides and Release Notes	~90 minutes

	• Questions and Answers • Etc.	
Administration Overview	Pre-requisite Training Basic User Training Reporting Overview	~60 minutes
	Focused for those end users who will be administering the system, such as but not limited to: • Admin Tab Overview and Features • Creating User Accounts and Account Templates • Asset Vehicle Folder Structure • Alerts • Linking assets • Viewing user history • Help, User Guides and Release Notes • Question and Answers • Etc.	

***Duration:** Estimated time depending on the client's requirements

Onsite System Training: This deliverable provides onsite training by qualified SkyHawk Telematics staff to the Client training personnel and management for the use and administration of the system. Training will be provided based on the Client personnel job responsibilities and their interaction with ConnectAnywhere and the various system components. SkyHawk's software training specialist will provide on-site training and will provide full product training as well as training printouts for participants for the full group of admin users in conjunction with installation.

The training solution includes the provision of all required digital and print materials. SkyHawk will provide the comprehensive set of training manuals in both digital and hard copy for the Operation, Diagnostics and Service & Repair for all aspects of the system.

Below is a high-level training topic list that will include the following topics and can be tailored to the Client requirements:

- A full Software tutorial for the End Users of the ConnectAnywhere web-based monitoring solution, including but not limited to:
 - Log-in & out of Account
 - Mapping interface features, including configuration for polygons
 - Reporting capabilities
 - Geofence creation
 - Asset Status features
- A full Software tutorial for the System Administrators of the ConnectAnywhere web-based monitoring solution, including but not limited to:
 - Creating assets and hardware records
 - User logins/account profiles
 - Hardware swap procedure
 - Decommissioning vehicle procedure
 - Hardware Installation & Troubleshooting training:
 - Wiring and wire routing
 - Hardware component installation and configuration
 - Hardware commissioning and test
 - Diagnostic and troubleshooting procedures
 - Retraining and Technical Support
 - Webinars on new features
 - Refresher training as needed
 - Assistance provided by Support Team
 - Support Contract info/hours

Hardware Install & Troubleshooting Training: Hardware installation and troubleshooting training will be conducted on-site to cover operations, diagnostics, installation, service, and repair, as per requirements. The SkyHawk installation approach encourages including the client's in the installation process to allow a hands-on training approach and to reduce the Client overall operational costs.

Equipment Installation, Diagnostics, Service & Repair: SkyHawk, will provide hardware installation and hardware troubleshooting/diagnostics training to the client's assigned fleet services team members. SkyHawk will offer a full installation certification training program to the Client Fleet Services dedicated staff. SkyHawk recommends that installation and troubleshooting training be conducted at the start of installations for Client mechanical staff to get a hands-on learning experience. The installation training will include hardware wiring and wire- routing, as well as hardware commissioning and testing procedures. Installation and hardware troubleshooting documentation will also be provided for reference.

Product Training: Our training programs are designed to ensure all user groups of the SkyHawk Telematics offerings obtain maximum value from the user experience. Programs include on-site & remote web-based training utilizing a variety of methods including software, videos & printed resources.

Prerequisite/Basic Knowledge Concepts (Mechanic Installation Training): The following are, but not limited to, basic prerequisite and basic knowledge requirements of the client's mechanics and installers. Mechanics should already be familiar with:

- Shop Safety and First Aid
- Fire Safety
- Vehicle Safety (especially working under the hood, moving vehicles)
- Knowledge and use of appropriate PPE (personal protective Equipment)
- Basic Electrical knowledge - voltage, current, resistance, series and parallel circuits
- Use of test equipment – multimeters, continuity testers
- Continuity testing and electrical troubleshooting techniques
- Wire Gauge selection
- Electrical Components familiarity – resistors, fuses, relays
- How to make proper electrical connections (soldering techniques, crimps)

The client's Mechanics/Installers should have an awareness of the following, but not limited to, the following vehicle concepts (SkyHawk can also aid/coaching):

- Vehicle battery familiarity, safe operating procedures, and testing
- ECM port identification and differences (OBD2, J1939, J1708)
- Fuse panels and fuse identification
- 12 and 24-volt vehicle systems, frame grounds
- Wire pulling techniques
- Exposed wire protection (shrink tubing application, electrical tape application)
- Antenna placement (cellular/GPS and satellite)
- Quality installation techniques:
- Proper wire routing/placement (raceways, panels, floorboard access)
- Split loom usage
- Tie wraps
- Surface cleaning for adhesive installation

Re-training: As part of the training package, SkyHawk provides the client with comprehensive training materials allowing personnel and management to refer to the tutorials at any time by simply clicking a link. The tutorial package consists of screen-flow diagrams with text, to allow users to select their preferred learning program.

The sales and technical teams at SkyHawk are very active in participating in and attending relevant technical and AVL events to ensure that we offer cutting-edge, competitive technologies. SkyHawk will provide training on any major software features changes, via webinar sessions at no additional cost for the duration of the contract.

- The following documents will be provided to assist with training:
- Installation manuals
- Hardware Diagnostics & Repair manual
- System Operation manuals

Web-based System Training: In addition to initial onsite training, SkyHawk also recommends the Client participate in a follow-up webinar training session 2-3 week following installations when the system has the newly installed vehicles set up and is fully functional. This training consists of web-based remote training to all system users to familiarize them with the usage and functionality of the ConnectAnywhere monitoring website. These sessions are intended to reinforce initial training. Each session can support up to 50 online trainees.

Post-implementation, software, diagnostics, install, service and repair training will be conducted twice per year by SkyHawk training staff and is recommended to be done once in the fall before winter activities, and again at the end of the winter season. Further, SkyHawk will also provide webinar training on a quarterly basis to unlimited users, to refresh, train new employees and cover any major software feature enhancements/changes.

Training Documentation: As part of the training package, SkyHawk offers a comprehensive software training guide, allowing the Company's personnel and management to reference any feature within the system. SkyHawk will provide the client with training on any major software features changes, via webinar sessions at no additional cost for the duration of the contract.

Hardware Documentation: All documentation required for understanding the hardware, installing, troubleshooting, and for performing repairs shall be provided to the client by SkyHawk.

Training and Workshop Schedule/Timelines: SkyHawk shall collaborate with the client to produce a reasonable schedule and accommodate the training.

h. On-going support and enhancement over the life of the agreement

The transition from project implementation to Operational Support (post go-live) is part of the Project Closing phase of a project. All in-scope AVL devices and in-scope peripherals have been installed, tested, and are successfully reporting in ConnectAnywhere. The system has completed the UAT and operating as expected. Once the last installation is completed, the Project Manager will send a communication to the City that the project is now entering the Closed phase and will be transferred to the assigned Account Manager and Operational Support. They are responsible for the following ongoing support items:

Account Manager:

- Schedule additional ConnectAnywhere user training and coaching
- Share new hardware/software features and functionality
- Ordering of hardware
- Request changes to data plans
- Billing inquiries
- General inquiries
- Escalation of unresolved issues to the management team

SkyHawk Support Desk:

- Technical support and troubleshooting
- Installation support and testing
- Dispatch service call visits

- ConnectAnywhere user support (password reset, account adjustments, etc.)
- General inquiries

For ongoing support, the SkyHawk Support Desk will assist the Customer with troubleshooting malfunctioning hardware devices. If the device can't be fixed through Over the Air (OTA) configuration changes, manual reprogramming or additional diagnostic measures, the SkyHawk Support Desk will recommend either returning the device to SkyHawk for repair or dispatch a field technician for a service call.

The Customer shall contact SkyHawk Support Desk when making the following configuration changes:

- Baseline odometer or engine hour value
- ECM type
- Change to vehicle voltage of ATrack device
- Change to installation method of ATrack device (3-wire, hardware ignition only, or ECM power)

Installation, Removal or Repair of Hardware: The Customer shall contact the SkyHawk Project Manager or SkyHawk Support Desk to schedule a service call if a unit is to be removed, installed, or needs repair. SkyHawk will dispatch a trained, qualified service technician to the Customer site. SkyHawk technicians are equipped with a small stock of commonly used spare parts so they may complete a repair during the same service call as the initial troubleshooting. Equipping our Service Technician with spare parts results in both time and cost savings for the Customer.

Re-Order of Hardware: The Customer shall contact their SkyHawk Account Manager to place an order for hardware. A quote will be provided for the Customer's review and approval. A P.O. is required from the Customer to authorize the purchase.

Winter Hardware Validation Testing: SkyHawk will assist the Customer with training and a test plan to efficiently conduct its own Winter Hardware Validation Test to ensure the winter equipment is re-installed correctly and operating as expected. This test is encouraged every fall before the start of the winter season. SkyHawk can also provide trained technicians to conduct the test for an additional fee.

Return Material Authorization (RMA): The Customer shall contact the SkyHawk Support Desk to obtain authorization before returning any defective or un-used hardware. The SkyHawk Support Desk will respond in writing with the RMA number, return address and instructions for preparing the courier documents.

Discontinued Hardware: When a hardware device is to be discontinued, the SkyHawk Account Manager will notify the Customer in writing of the discontinued product and will provide as much advance notice as possible. A suitable replacement will be recommended by the Account Manager with an accompanying price quote. The SkyHawk Support Desk will provide an installation guide and assistance to install the new device for a demo period or can arrange for a service call to have the new device installed by the SkyHawk approved installation sub-contractor.

Communication

Regularly Scheduled Software Release and Maintenance Update: The SkyHawk Support Desk will notify key personnel of the Customer via email five (5) business days in advance of an upcoming Software Release and Maintenance Update. The first notice will include the date/time and approximate duration of the maintenance window. A reminder email is sent the day of the update and this notice will include the release notes. Once the update is complete, the release notes can also be found on ConnectAnywhere under the Help menu.

Service Interruption or Unplanned Outage: The SkyHawk Support Desk will notify key personnel of the Customer via email as soon as possible when any service interruption or unplanned outage of the software is detected. The Support Desk will continue to provide regular updates via email until the issue is resolved.

Annual Meeting: At a minimum, the Customer and SkyHawk will meet twice annually; in October to prepare for the upcoming winter season and then again in April to prepare for summer operations. Items on the agenda will include:

- Review any major software updates to the system
- Determine if any additional system training is required
- New hardware requirements (spare parts and/or new kits)
- Requirements for Installation Service (service calls and/or new installations)
- Vehicles that require suspended service (to be discussed in the spring meeting)
- Review of any outstanding Support Tickets/Issue Log

SkyHawk Support Personnel

SkyHawk Support Team: SkyHawk's Technical Support Team works closely with the Project Management Team and Installation Technicians to offer deployment and post-sales support to our Customer base. Customers can reach the Support Desk via a toll-free support line 1-844-424-7759 ext. 2 or by sending an email to support@skyhawk.co. All issues that are emailed to support are automatically logged as a ticket in the JIRA issue management system. Level 1 Support is the initial point of contact provided by SkyHawk. Any issues that can't be resolved by Level 1 are forwarded to the Level 2 Development Manager to assign the appropriate resource for resolution.

Level 1 Support: SkyHawk's experienced frontline Level 1 Support Team product specialists handle the lion's share of the trouble tickets on a day-to-day basis. Level 1 can assist with website and report issues, system administration, hardware configuration, installation support and hardware diagnostics/troubleshooting. All issues reported to Level 1 are logged in the Jira issue-management system and triaged based on severity outlined in our Service Level Agreements. Support resources will make every effort to resolve the issue as quickly as possible. Issues that can't be resolved by Level 1 Support are escalated to Level 2 Support.

Level 2 Support: Is comprised of a team of highly skilled software developers and hardware engineers located in SkyHawk's head office in St. John's, NL. Level 2 support will evaluate the issue and advise the SkyHawk Project Manager/Account Manager of the expected resolve date, who will communicate back to the Customer's Project Manager and/or the person who raised the ticket. Issues that are considered low risk may be implemented into the production environment as "Hot Fixes", while fixes that require more development effort and testing are scheduled for implementation into a regularly scheduled maintenance release, which typically takes place once per month.

The SkyHawk Support Team is available 8:30 am – 5:00 pm, Monday through Friday for email and telephone support. Emails are not monitored outside of business hours however Telephone support is available 24/7/365 for Critical Issues classified as Priority 1 or Severity 1.

After Hours Response for Critical Issues: Any issues called into the Technical Support Line outside of SkyHawk business hours are automatically forwarded to the Telalink call centre that operates 24/7/365. Any issues that cannot be resolved by Telalink and are determined to be critical in nature are escalated to the appropriate personnel via the emergency call-out procedure. Examples of critical issues are website down/users cannot log in, or the system is up but the vehicles are not updating with live data. SkyHawk will take appropriate actions and pull together the resources necessary to resolve critical issues as quickly as possible. Any non-critical issues are deferred to the SkyHawk level 1 support team to address the next business day.

Account Manager: After the project implementation is complete, the Account Manager will take on the role of the Customer's main point of contact for any issues besides regular ongoing support. The Account Manager is responsible for ensuring the Customer is kept up to date on the software development roadmap and new hardware technologies. The Account Manager is also responsible for providing quotes when reordering hardware or sourcing new products, establishing regular meeting intervals, and coordinating training as required.

4 - Service Factors:

a. Description of related services included in Turnkey Solution

SkyHawk Telematics has been delivering advanced telematics solutions to government mixed fleet, including winter operations functionality, for more than 10 years, to clients in the USA and Canada. Our continued focus on being the industry leader in this sector and in working with our clients has produced functionality which includes:

- integration with most major material spreader controllers,
- cost-based reporting for material usage,
- winter operations trip & material usage reports,
- public winter ops site,
- in-cab route optimization,
- route navigation and return-to-route,
- route activity reporting,
- blade wear report,
- spreader speeding,
- direct liquid application (DLA) report, and much more.

The SkyHawk System, ConnectAnywhere, is a web-based monitoring solution designed for enterprise level, cloud-based service which facilitates the real-time visibility and management of an organization's valuable assets. The service provides unique asset identification, GPS location and vehicle status integration with sensory information such as plow, spreader, PTO, beacon, and brooms.

As the name implies, users of the ConnectAnywhere system only require an internet connected computer or mobile device with a supported web browser to access information most anywhere in the World.

As an end-to-end solutions provider, with a proven track record of successful client partnerships, we understand the needs of complex deployments.

SkyHawk's ConnectAnywhere web-based monitoring solution is hosted out of AWS Data Centre guarantees 99.9% service availability, 24/7 onsite support, automated system monitoring and dynamic resource allocation controls. For instance, as more network bandwidth, CPU, RAM, storage is required, the system dedicates the necessary computing resources. Furthermore, the solution provides a separate dedicated database, virtual server, IP address and SSL security. These dedicated resources ensure the highest level of performance and that the system is not degraded by other companies sharing the same system resources.

ConnectAnywhere allows unlimited user accounts or logins with Skyhawk staff providing the initial account setup and administration. Once the system is fully operational, clients have complete administrative IT access to the features and functionality of the system. The ConnectAnywhere solution provides complete GIS mapping integration and interface capabilities to other client software applications with REST API.

Some key features of the SkyHawk solution include:

- The ability to obtain ECM engine data including fuel efficiency characteristics such as: Total Fuel Used (L),
- Fuel Rate (L/h), Instantaneous Fuel Economy (km/L), Average Fuel Economy (km/L) when available from the vehicle manufacturer.
- The ability to report on unsafe driver actions such as speeding (with local speed zone), harsh braking, harsh acceleration, etc.
- Alerts and alarms that are configurable and which can be delivered directly to users via email or SMS messaging
- Unlimited number of user accounts (usernames and passwords) with complete administrator level access and system control, multiple user access levels (e.g. Viewer, Manager, Admin, etc.) controlled by administrator

- Create email and text contact lists per asset for real-time notifications
- Map options default to Google but access to client maps via ESRI/GIS link
- Website protected with industry- standard 128-bit encryption with an SSL certificate Ability to filter vehicles in real-time and the view of the data online
- Custom Geo-Fencing and alerts on activity in and out of Geo-Fenced areas Zoom-In, Zoom-Out, Pan, Drag- Zoom, Road Map Data, Air-Photo Data, etc. Access to reports in real-time online.
- Optional - Tablet support for in- cabin operations supporting advanced navigation and routing options.
- Optional - A completely integrated satellite asset tracking support for vehicles and for high valued, non-powered assets.

Our solution can integrate with other software and IT applications and is built on one of the most advanced networks and computing platforms available, providing a long-term solution to our customers. Thus, our telematics solution will meet, and in many cases exceed, all aspects and requirements of the organization.

The SkyHawk solution is provided to our clients as a monthly online service and not as "Software" in the traditional sense. Customers will not have to install any programs, routines, scripts etc. or run any software to use the SkyHawk ConnectAnywhere solution. All you need is a modern browser and an internet connection.

SkyHawk Telematics is device agnostic. We pick the best hardware manufacturers from around the globe to address each vehicle type requirements, from simple track-and-trace, to complex spreader integrations, to vehicles with multiple IO requirements.

Each piece of hardware is selected to perfectly fit each vehicle's specific requirement and not one piece of hardware is made to fit all. Partnering with multiple hardware vendors also means that we are able to offer our clients the most current and up-to-date hardware, ensuring that we future proof your solution by not only meeting their requirements for today but being flexible to anticipate and meet future requirements.

The modems we offer have a robust set of features with reliable track records, including standard store- and-forward capabilities for when the vehicle is out of cellular coverage, as well as the ability to receive and perform over-the-air (OTA) configuration or firmware updates in the field.

This eliminates the need to physically visit the vehicle for support and maintenance.

SkyHawk's most widely used modems range from simple track and trace to the most complex of applications used for optimal winter maintenance tracking.

As an end-to-end solutions provider, with a proven track record of successful client partnerships, we understand the needs of complex deployments.

Experienced and competent subject matter experts: SkyHawk has a team that has successfully delivered similar projects of scope and scale. SkyHawk's team includes senior management/corporate project sponsors, sales account managers, project management specialists, operations/procurement/order fulfillment staff, installation teams, support staff, and financial/billing specialists.

Project Management: Effective management is vital to the overall success of any project and SkyHawk has proven its ability to deliver telematics projects to complete vehicle and feature roll with very large and complex projects.

Project Management Approach: Skyhawk's Project Team utilizes the Project Management Institutes (PMI) project methodology phased approach that is broken down into five (5) process groups: Initiate, Plan, Execute, Monitor and Close. In each process area, we have identified key documents and tools to serve as inputs that result in deliverables for each phase.

SkyHawk's project team will spend a considerable amount of effort on detailed requirements gathering to ensure a complete understanding of the Client's needs and will compile a comprehensive Project Plan which we feel is critical to the project's success. The Project Plan will be updated regularly as the project progresses, and will establish project roles and responsibilities, a detailed schedule of tasks, Quality Plan, risks, and Change Control. Additionally, SkyHawk's project team will work with the Client's project team in preparing a full updated project schedule, including the Client's installation

schedule. Bi-weekly status meetings will be held to review the project schedule and to review any open issues in SkyHawk's JIRA ticketing system.

Project Communication: Project Communication will be established in the form of regularly scheduled project meetings with status reports issued weekly. The status report will contain at a minimum the following information:

1. Dashboard view on the progress of installations, tracking completed installs to planned
2. Task / Action Item List from previous meetings
3. Defect /Issue Log generated from the Jira Ticketing System
4. In addition, SkyHawk will collaborate with ODTO on preparing awareness communications for ConnectAnywhere training, hardware installation training, etc., as appropriate.

Communication Plan: The Project Communication plan will be created in partnership with SkyHawk and the client's Project Managers to outline how the AVL project team will be communicated during the project.

The Communication Plan shall be completed early enough in the project to be included for review at the Project Kick-off Meeting. Communications include but not limited to; status, meetings, issues, deliverables access, and design/document reviews.

Reporting Methods: SkyHawk, in collaboration with our client's project team, shall determine reporting and communication cadences. During the project implementation phase, the Status Report will be issued weekly or bi-weekly, prior to the Project Team Meeting. The Status Report will contain percentage complete and dashboard views of scope, schedule, cost, and quality. It will be prepared in formats approved by the client and will contain at a minimum the following information:

1. Progress Dashboard showing percentage complete from previous meetings
2. Defect Log generated from the Jira Ticketing System
3. Project Status as it relates to the Work Plan
4. Deliverables status
5. Planned activities for the upcoming two (2) week period
6. Future activities
7. Requirements Traceability Matrix (RTM)
8. Report and remedies in case of falling behind Schedule
9. User Acceptance Test Feedback
10. Risk/Action/Issues/Decision (RAID) Log

Solution Configuration: SkyHawk's "ConnectAnywhere" solution is the result of our unwavering commitment to our client partners to provide them the data they require to make informed decisions to maximize operational efficiency, minimize environmental impacts, and protect the safety of both employees as well as the general public. Through continual consultations with the people responsible for the wellbeing of municipal, provincial, and state fleets and the roadways on which they operate, we have incorporated the feedback of these industry experts, along with the lessons we have learned along the way, to the data we collect and the information we report.

To accommodate the ever-increasing volume and diversity of data sources we pull from, the latest version of ConnectAnywhere is architected using modern design techniques that allow us to support many thousand simultaneous connections while maintaining flexibility through the use of the schema-less MongoDB database. This provides us the capability to add or modify the underlying data of ConnectAnywhere to support new feature development without the complexity and downtime that would be required in a more traditional relational database environment.

This flexibility also allows us to support a wide variety of data collection devices, including multiple models of spreader controllers, telematics modems, asset trackers, etc. which enable us to provide a "right-sized" solution for the highly diverse fleets our clients maintain. We also promote "configuration" over "customization"; when we are presented with a business problem to address for one of our client partners, we approach the solution in such a way to benefit all of our users, with consultations as necessary, and make the additions available to our entire client base with the capability to adjust parameters to suit their own operational needs

The client onboarding process involves our project team gaining a thorough understanding of our client's business requirements, which is then used in the setup of your ConnectAnywhere portal. Starting with the master vehicle list, we

painstakingly review every vehicle and the data points to be collected from each, including such items as the ECM type, spreader controller, discrete inputs for plow blade position or beacon light monitoring, etc. This is then entered into ConnectAnywhere, which allows us to normalize the potentially many different sources into the consistent user experience in terms of display and reporting. From there, we can adjust the vehicle messaging profile and event thresholds to suit your business goals. We also work with you to gather the user account information to create the "account templates" that control the functionality and subset of assets that each end-user has available to them. Other key configuration items include the setup of system alerts and scheduled reports.

Specialized Solution Offering: When dealing with a complex fleet of mixed vehicles with specialized reporting functionality (e.g. winter operations) it is very important to acquire a solution that is designed and built for the vehicle types and operations of a large municipal organization. SkyHawk's ConnectAnywhere telematics solution has been designed and built specifically for this application and supports the specialized and advanced functionality required to operate these services more effectively and efficiently.

Installation Plan/Staff: Vehicle installations and testing are one of the most critical parts of any telematics system. At SkyHawk we refer to it as the "foundation" upon which all other functionality is built or layered. A well-designed installation plan along with a team of reliable installers is required for success. Furthermore, it has been the experience of SkyHawk that best results are achieved when a combined approach of vendor/contracted installers working in conjunction with our client's mechanics and technical staff is utilized.

Effective Communications Plan: Engagement of the client's staff and departments to obtain a deep understanding of goals and objectives, as well as obtaining input, feedback, and required "buy-in" from management, system users and stakeholders leads to a better managed and implemented solution. This is best accomplished with an effective communication and engagement plan which starts before implementation begins and carries through all project phases. SkyHawk has significant and relevant experience working with large clients in delivering successful communication plans.

Project Team: SkyHawk has assembled a team of experts in the deployment of AVL projects. They are motivated by excellence and have the combined skills and capabilities to deliver the project on time and on budget and of the highest quality.

b. Experience and qualifications of partners and subcontractors

SkyHawk owns and has designed and built the cloud-based telematics software solution however a technical partner ecosystem is utilized for various aspects of our solution including the cloud-hosting, database managed services, mapping interface, in-vehicle data collection and communications hardware as well as interfaces to other third-party software applications as may be required by the client.

SkyHawk's partnerships, which support our main ConnectAnywhere cloud-based application, mainly consist of large, leading enterprise-based organizations such as Google, MongoDB and Amazon (AWS). The other major component of our technical partner ecosystem includes the companies that provide physical hardware included telematics modems, cabling and sensors which collect and transmit data from the vehicles. To ensure we are not exposed to any major supply chain issues (including those caused by COVID-19) SkyHawk holds a significant inventory of most all its major components for rapid and easy distribution to our clients.

Over the past 10 years SkyHawk has a holistic approach and developed a strong working relationship with selected partners and subcontractors to bridge the gap in offering our clients a comprehensive, one stop solution. An example of our success with partnering is for the City of Pittsburgh. As part of a public bid award, SkyHawk partnered with Quetica LLC, and Magellan Solutions provided the City of Pittsburgh with a complete Telematics Solution, Route Optimization, and Route Navigation system. 138 winter vehicles were installed in Phase 1 of the project during Q4 2018, with a mix of approx. 350 heavy and light-duty installation during Phase 2 of the project in Q4 2019.

Sensor integration to monitoring a variety of inputs including lights, plow blade up/down, etc. were incorporated into the solution offering as well as integration with spreader control systems to provide detailed data reports on

salt, sand, and liquid utilized during winter operations. SkyHawk's partners will also be providing a new winter operations dynamic routing system to maximize efficiency in both plowing and spreading times.

The City of Pittsburgh has estimated that due to the use of their telematics project, they reduced their salt consumption by 60% for the Winter 2019 season when compared to Winter 2018 using pounds of material spread/per inch of snow calculation, for a savings of \$1.3 million.

c. Description of Additional Integration and Consulting Services provided

Vendor solution engineering/customization: While having specialized and feature matched system functionality is very important it is also important to have a telematics vendor that has the resources and capabilities to perform solution engineering. Our clients ultimately have requests and requirements which need custom development and attention to properly integrate with existing technologies and systems, including data exchange with other software applications. This cannot be achieved with "out-of-the-box" functionality. SkyHawk has a team of solution specialists and software engineers that can perform such tasks. Our clients have direct access to the Company who owns, designs, and develops the solution and not a solution reseller.

Rest API: ConnectAnywhere uses a REST API to easily integrate into third-part applications. The REST API provides simple read-only access to the most important data items in the ConnectAnywhere database, assets (both static attributes and current dynamic state) and messages (data points or transactions). It is an HTTP-based interface implemented using REST (Representational State Transfer) principles, intended to be used by application developers who wish to transfer asset and message data to third-party systems or data management tools. By using JSON and HTTP/HTTPS the API can easily be accessed by an application using any of a variety of languages. The API is not event/notification based.

SkyHawk Telematics - SERVICE LEVEL AGREEMENT (SLA)

This “**Service Level Agreement**” is made pursuant to the AGREEMENT between Client (Buyer) and SkyHawk Telematics (as defined therein, the “**Agreement**”), to which this Service Level Agreement is attached as a Schedule. The terms of the Agreement are incorporated herein by reference. All capitalized terms not defined herein, shall have the meanings set forth in the Agreement. Actual Services must be separately acquired and paid for this Service Level Agreement to apply to any use of the Services.

1. Description of Services

1.1. Definitions – The following terms are defined for the purposes of this Service Level Agreement only:

- (a) “Critical” means any performance, operational or quality issues with BOSS Services, which result in the inability to use any of the BOSS Services for an extended period.
- (b) “Error” means any Failures or other performance, compatibility, operational, or quality issues, which result in the BOSS Software or Services not operating in accordance with the Agreement or the applicable Documentation and/or Specifications. An Error may have no appreciable impact on the operation or use of the BOSS Software or Services, or an Error may cause a “Minor Failure”, “Serious Failure”, or “Critical Failure”.
- (c) “Error Correction” means creating a permanent modification to the BOSS Software that enables the permanent resolution of an Error, implemented with an Update, Upgrade or Version. Error Corrections are implemented according to a BOSS testing, BOSS acceptance and BOSS implementation schedule.
- (d) “Help Desk” means BOSS’s telephone support line.
- (e) “Help Desk Services” means the telephone and service level management services provided by the Help Desk as described herein but excludes Training Services.
- (f) “Minor” means any performance, compatibility, operational, or quality issues that are not Critical Failures or Serious Failures. Minor failures can be an Error that does not interrupt critical workflow, are cosmetic in nature, or any Error for which a workaround is available.
- (g) “Patch” means the temporary repair or replacement of object or executable code versions of the BOSS Software on its production server(s) that enables the temporary resolution of an Error.
- (h) “Serious” means any performance, compatibility, operational, or quality issues with the BOSS Software that cause disruption to normal workflow and for which BOSS cannot provide a workaround. Serious Failures can be intermittent server downtime, user accessibility issues, or inability to access a key system function.
- (i) “Software Support and Maintenance Services” means the BOSS Services provided pursuant to Section 3 of this SLA.
- (j) “Update” means any new minor enhancement made to the BOSS Software issued by BOSS, which may also contain an Error Correction, and includes any update, patch installation, modification, renovation, refresh, enhancement, addition or substitution to the BOSS Software. Updates will be identified with a new update series number; for example 2.1.1 to 2.1.2.
- (k) “Upgrade” means any new major enhancement or grouping of enhancements, new functionality or revised or new modules made to the BOSS Software, issued by BOSS, and includes a collection of one or more Updates released as an Upgrade. Upgrades will be identified with a new Update series number; for example 2.1.2 to 2.2.0.
- (l) “Version” means any release of an Upgrade or collection of Upgrades to BOSS Software in respect of which BOSS uses a new version series number; for example 2.2.0 to 3.0.0
- (m) “Workaround” means a change in the procedures followed by Customer to avoid an Error without substantially impairing Customer’s access to or use of the BOSS Software.

2. Help Desk Services

2.1. The Help Desk Services set forth in this Section 2 of the SLA (the “**Help Desk Services**”) are provided in the categories indicated, based upon the selection of such BOSS Services in a Purchase Order, and payment of the applicable Service Fees in accordance with the Agreement.

2.2. BOSS shall staff a telephone Help Desk to provide assistance regarding the function, operation, and use of the BOSS Software, the Services and the Products, including:

- a) Reporting of issues;
- b) Assistance with diagnosing and resolving issues,
- c) Provision of Workarounds,
- d) Assistance other technical questions concerning the operation, maintenance, and use of the BOSS Software (but not training).
- e) In the event the Help Desk cannot resolve the issue, reference of the call to BOSS through the opening of a support ticket.

- 2.3. The Help Desk is available Monday to Friday 8:30am to 5pm EST or via email support@skyhawk.co . After Hours - call toll-free number below for the critical issues. Those calls will be dispatched to support personnel. Issues emailed to support after hours will be responded to next business day.

(a) North America: Toll-free number 1-844-4-24-7-SKYHAWK (1-844-424-7759) extension #2

3. **Service Response**

- 3.1. BOSS tracks customer reported issues and requests with support tickets. Each issue is assigned a support ticket with a unique identifier.
- 3.2. BOSS business days are 8:30 am to 5:00 pm EST, Monday to Friday, excluding Ontario statutory holidays.
- 3.3. For each support ticket for which BOSS identifies an Error as the cause, BOSS shall provide a Workaround or Patch and Error Correction in accordance with the guidelines in the chart below:

Error Severity	Acknowledgement	Response Time	Resolution
Minor	Upon Distributor or End Customer call to Help Desk or receipt of reply email from BOSS	BOSS shall respond within 1 business day	At the discretion of BOSS, will provide a Workaround and/or Error Correction in the next Version, Upgrade, or Update.
Serious	Upon Distributor or End Customer call to Help Desk or receipt of reply email from BOSS	BOSS shall respond the same business day, or if outside BOSS business hours, the next business day.	BOSS shall provide a Patch within 5 business days following response if possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.
Critical	Upon Distributor or End Customer call to Help Desk or receipt of reply email from BOSS	BOSS shall respond the same business day, or if outside BOSS business hours, will attempt to respond ASAP, but in all cases within 1 hour the next business day.	BOSS shall provide a Patch as soon as possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.

- 3.4. Distributor, on behalf of each End Customer or End Customer agrees to provide BOSS with all reasonably available information and materials requested by BOSS for use in replicating, diagnosing and correcting an Error reported by End Customer. End Customer must be using an Internet browser supported by the BOSS Software and must have continuously paid for Support and Maintenance Services acquiring the Service.
- 3.5. BOSS shall use commercially reasonable efforts to release Updates in a timely manner so as to keep the BOSS Software current with changes in operating systems, widely adopted Internet browsers, and other key computing platform elements on which, or in connection with which, the BOSS Software is used.

4. **Exclusions**

- 4.1. The BOSS Services provided hereunder shall not include:

- (a) Training Services;
- (b) Migration of data to or from other fleet and asset tracking systems; or
- (c) Custom Development Services,

which additional services may be provided pursuant to separate Quotation.

- 4.2. BOSS shall not be obliged to perform, and may suspend performance of, the BOSS Services, in the following instances:

- (a) Distributor or the End Customer has modified the installation environment of the BOSS Software, Products or Services without consent;
- (b) Distributor or the End Customer is in material breach of the Agreement, including failure to pay;
- (c) Distributor's or the End Customer's installation environment fails to meet the minimum requirements for the BOSS Software as set forth in the application Specifications; or

- (d) Distributor and the End Customer refuse to provide the necessary information to duplicate and/or assess the severity of the Error.

5. Service Level for SaaS Products (99.9% SLA)

This Service Level Agreement (the “SLA”) governs the use of all network infrastructure products and services (collectively, the “Services”) offered by SkyHawk Telematics, its parent company, and their affiliates and subsidiaries to its customers (“Customer”).

- 5.1. Service Commitment. SkyHawk Telematics is committed to providing services to its Customers at a standard of excellence commensurate with the best practice in the industry. Network uptime and server availability are of the highest importance. The following service levels are designed to assure Customers of ultimate performance and maximal uptime.
- 5.2. Server Hardware Replacement. SkyHawk Telematics guarantees the functioning of all hardware, including servers, CPU’s, cabling and associated server hardware, firewalls, load balancers, and storage area networks, and will replace any failed component at no cost to Customer within two hours following SkyHawk Telematics’ notification of the failure and SkyHawk Telematics’ identification of the failed hardware (the “Replacement Guarantee”). “Hardware” means the Processor(s), RAM, hard disk(s), motherboard, NIC card and other related hardware listed in the Service. The Replacement Guarantee does not include the time required to rebuild a RAID array or the reload of the operating systems and applications or changes to hardware during Maintenance, as defined below.
- 5.3. Power and HVAC Availability. SkyHawk Telematics guarantees that its power and HVAC systems will be available 100% of the time in a given month, excluding Maintenance, as defined below. “Infrastructure Downtime” means: (a) the SkyHawk Telematics power or HVAC systems are not available and (b) Customer submits a SkyHawk Telematics trouble ticket detailing the unavailability of the SkyHawk Telematics power or HVAC systems resulting in Customer downtime. Infrastructure Downtime does not include downtime issues related to power supplies on Customer’s servers, load balancers, or switches.
- 5.4. 99.9% Network Uptime. SkyHawk Telematics guarantees that the SkyHawk Telematics network will be available 99.9% of the time, excluding Maintenance, as defined below. Customer is eligible for a credit for Network Downtime for any breach of this guarantee, which can be verified by SkyHawk Telematics technical support team. “Network Downtime” is defined as an inability to transmit and receive data caused by failure of network equipment supplied by SkyHawk Telematics, excluding Maintenance, but including managed switches, routers, and cabling, and specifically excludes failure of network equipment and infrastructure owned or operated by the Public Switched Telephone Networks, cellular providers and/or satellite providers.
- 5.5. Maintenance. “Maintenance” means Scheduled Maintenance or Emergency Maintenance. “Scheduled Maintenance” means any maintenance in the SkyHawk Telematics datacenter of which Customer is notified at least 5 days in advance. “Emergency Maintenance” means any maintenance in the SkyHawk Telematics datacenter that: (a) in SkyHawk Telematics’ sole discretion, is necessary to avoid an immediate threat to the SkyHawk Telematics datacenter or Customer’s server and (b) of which Customer is notified.
- 5.6. Remedies. In the event SkyHawk Telematics fails to meet the Replacement Guarantee or customer experiences Infrastructure Downtime or Network Downtime as outlined herein, provided Customer follows the procedures outlined herein, SkyHawk Telematics will apply a credit (“Credit”) to Customer’s account in an amount equal to five percent (5%) of the Net MRC for the affected account for each hour of downtime or fraction thereof. “Net MRC” means the monthly recurring charge for the service, excluding cellular or satellite telecommunication fees, for the units impacted by the server(s) experiencing the issue(s). The Credits described in this SLA will be Customer’s exclusive remedy and SkyHawk Telematics’ entire liability for any breach of any warranty of performance or service contained in this SLA. In order to claim Credits, Customer must open a SkyHawk Telematics trouble ticket. All downtimes will be measured from the time the ticket is received and validated by SkyHawk Telematics to the time SkyHawk Telematics, in its sole discretion is able to resolve the issue. Customer may not receive more than one Credit per affected configuration per incident and in no event will Customer receive greater than one month’s Net MRC in Credit for any given month regardless of the number of incidents. Customer must be a SkyHawk Telematics customer in good standing to receive the Credit. No Credit will be applied to accounts that are past-due or for accounts that are canceled before the conditions for payment of the Credit are met. Upon cancellation of the Customer’s account, any outstanding or previously accrued Credits will be forfeited. Credits will be applied against purchases or renewals for which payment is due after the date the credit is applied. Credits will not be applied against past due balances.
- 5.7. Exceptions. Customer shall not be entitled to any Credit hereunder if Infrastructure Downtime or Network Downtime is caused by: (i) actions of the Customer or others authorized by Customer to use the Service under the Agreement; (ii) failure of applications or other software not provided by SkyHawk Telematics, (iii) the result of Maintenance activity, (iv) Denial of Service attack, hacker activity, or other malicious event or code targeted against SkyHawk Telematics or a SkyHawk Telematics Customer, or (vi) failure of any Network or Internet Infrastructure not owned or managed by SkyHawk Telematics. Server Hardware Replacement guarantee does not include time required to perform data restores and backups if applicable.

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory H: Snow & Ice Removal and Route Management

Subcategory O: Utility Operations, Monitoring and Support

Client Company name:	Skyhawk Clients, various, see below.
Client name of contact:	Response below
Client contact title:	Response below
Client is a daily user, occasional user, etc.:	Response below

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Chris Stokes no later than Friday, November 6th.

Thank you for your assistance in this process.

- 1. For what services do you use USCC's product, and how long have you been USCC's customer?**

Responses below.

- 2. Would you recommend USCC to other customers? Why?**

Responses below.

- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

Responses below.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

Responses below.

- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

Responses below.

- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

Responses below.

- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

Responses below.

- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

Responses below.

The following are a sampling of some governments clients that currently use the SkyHawk solution:

City of Portland, MA	North Dakota DOT
Town of Davenport, IO	Nova Scotia DOT
Town Urbandale, IO	County of Grande Prairie, AB
Rochester Hills, MI	City of Red Deer, AB
Midland County, MI	Federated Co-op, SK
Muskegon CRC, MI	Manitoba Hydro, MB
Midland CRC, MI	City of Hamilton, ON
City of St Clair Shores, MI	Hydro One Networks, ON
City of Kalamazoo, MI	Town of Flat Rock, NL
Stark County, OH	Hydro One Networks Inc., ON
The city of Brunswick, OH	Municipality of Chatham-Kent, ON
City of Joliet, IL	Hydro-Quebec, PQ

City of Springfield, MO	Town of Quispamsis, NB
City of West Fargo, ND	Town of Rothesay, NB
City of Pittsburgh, PA	Town of Dieppe, NB
City of Mount Pearl, NL	Portugal Cove-St. Philips, NL

Our references below will attest to SkyHawk's ability to deliver a superior product on time and in scope.

Reference (1)

New Hampshire Department of Transportation

7 Hazen Drive Concord, New Hampshire 03302-0483

David Gray

Winter Maintenance Program Specialist

(603) 485-3806 ext. 324

dgray@dot.state.nh.us

October 2016

Ongoing Project

GPS/AVL Winter Operations Solution. 65 Winter Operation Vehicles, and 24 Pickup Trucks - 89 Units

\$272,072.66

Reference (2)

City of Pittsburgh

414 Grant St. Pittsburgh, PA 15219

Chris Belasco

Project Manager

(412) 400-4505

chris.belasco@pittsburghpa.gov

October 2018

Ongoing Project

Complete Telematics Solution, Route Optimization, and Route Navigation system. 138 winter vehicles with a mix of approx. 350 heavy and light-duty vehicles - 488 Units

\$1.5 Million

Reference (3)

City of Hamilton

71 Main Street West, Hamilton, ON L8P 4Y5

Angela Storey

905-546-2424 ext. 6483

Angela.Storey@Hamilton.ca

April 2016

Ongoing Project

EMS vehicles that required integration with Bluetooth, Garmin devices for in-cab communication with Central Ambulance Control Centre and Ministry of Health and Long-Term Care reporting system as well as PTO reporting for lights, sirens.

Roads & Maintenance vehicles - design and creation of a Public access website, a mobile app for contractor specific application, integration to spreader controllers, and PTO status for winter snow plows.

Simple track and trace for Parks and Recreation, Animal Services, Buildings, By-laws, Cemeteries, Forestry, Hamilton Water, Horticulture - 750 Units to date.

\$5 Million

Reference (4)

Hydro One Networks Inc.

6975 Kenderry Gate | Mississauga, Ontario L5T 2Y1

Frank Currie

Manager - Fleet Services

(905) 696-7190 x 3315

frank.currie@hydroone.com

October 2013

December 2016

SkyHawk Telematics provided Hydro One with a complete telematics solution that facilitated fleet monitoring for multiple lines of business including Construction Services, Forestry, Provincial Lines, Fleet and Station Services. Over 5000 vehicles were installed with a dual-mode cellular/satellite solution to equip its fleet comprised of the boom truck, off-road and light-duty vehicles. The hardware installation and testing was a joint effort between the Hydro One mechanics and SkyHawk technicians, taking approximately 22 months to complete.

\$20 Million

Reference (5)

City of Davenport Iowa

226 West 4th Street, Davenport, IA52801

Art Bartleson

Director of Public Works Street Maintenance Supervisor

(563) 327-5114

abartleson@ci.davenport.ia.us

December 2015

November 2016

Installed SkyHawk 4G GPS/AVL system in late 2015 to replace an existing 2G system from another vendor. Davenport monitors their salt spreaders equipped with FA5100 and FA6100 controllers, graders, and supervisor vehicles. They use the live "Route Service" mapping overlay to monitor winter operations. SkyHawk has developed a printable route completion report for drivers coming on shift; testing at Davenport and other customers is helping developers maintain a timeline for an early fall release. City snow operations staff use SkyHawk to manage material usage, report costs and improve efficiency. Waste Department on boarded 2020 with 31 garbage trucks.

\$82,000.00

Appendix P

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Category I: Public Safety Systems

Team on the Run by StreamWIDE



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
Team on the Run by StreamWIDE
- b. General Application Area (i.e. Attachment V Sub-Category A through G, listed in table below)
Subcategory I: Public Safety Systems
- c. General capabilities provided
Team on the Run is a secured all-in-one communications tool for public safety organization that can be deploy on SaaS or on-premise. Clients can be installed on smartphones, tablets and PCs. All communications are reliable and secured to protect the public safety agents and to facilitate collaboration and response coordination.

Key Team on the Run Public Safety Features:

- Integrated contact list controlled by administrator; all contacts are synchronized with most updated contact information across the organization.
- Contacts can be organized in teams or departments following organizational structure
- Functional/response groups defined by administrator
- Administration function can be delegated to multiple administrators for large organizations
- Ad-hoc groups communication
- Secured messaging The application applies NIST FIPS-140 compliant ciphering suites (AES, RSA, SHA-256/SHA-384, ECDHE) to encrypt all communications with the service
- Securely share pictures and videos
- Broadcast messages when information shall be delivered massively and reliably
- Message read receipt
- Message acknowledgement to confirm reception and interpretation
- Mobile client for Android and iOS
- Emergency handling functions
 - o Emergency button included in client app, reachable at all times
 - o Locate person that initiated emergency
 - o Enable text and voice communication with emergency initiator

Web dispatcher function

- Web client with dispatcher user
- GPS location of contacts on map updated in real-time
- Fully synchronized mobile and Web clients
- Push-to talk and VOIP function on Web client
 - o PTT Channels
 - o Group calling
 - o Fast PTT connection from map to reach agents in certain area

Additional communication capabilities

- Secured Push-To Talk function on mobile clients
- Floor priorities
- Late call entry
- Secured VOIP calling function

- Geo-location tracking
- Video streaming
- Video calling
- Emergency call/Message (add-on fee per user per month)
- Lone Worker protection / Man down alert (add-on fee per user per month)
- My business process and forms for planning missions and checklists
- Integration with ruggedized devices such as Sonim XP3/XP5
- Integration with LMR radios (requires integration fees)
- Option to deploy solution on-premise (needs to be quoted upon request)
- Channel interworking between public safety organizations
- Priority and pre-emption option

For on-premise implementation StreamWIDE can provide a quote upon request for the Team On Mission platform which has similar capabilities to Team on the Run with mission critical and 3GPP compliant functions.

- d. Expected impact on cost/performance/functionality, etc.

Team on the Run impacts and enhances organizations' performance in the following areas:

Facilitate collaboration between public safety organizations

Facilitate secure sharing of multimedia with evidence with command center

Facilitate joint coordination

- Dispatcher Web console
- PTT group calling
- PTT channels

Mitigate or eliminate security breaches or information leak by avoiding the use of consumer messaging tools and designating an official communication tool like Team on the Run.

Enable fast response

- Locate closest staff to incident
- Communicate in real time

- e. Subcontractors/partners involved in delivering service

US Cellular distributes Team on the Run SaaS. Team on the Run is a product developed by StreamWIDE, StreamWIDE team is responsible for implementation (delivery) and support.

- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.

Yes. Please see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described

Team on the Run allows public safety organizations to:

- Facilitate public safety staff response communication coordination in a secured way

- o PPT group communications
 - o PTT multi-channel
 - o PTT channel interoperation between agencies
 - o Web dispatcher console with PTT capabilities
 - o Location of staff in console map
 - Increase situational awareness by locating other members of response team in mobile device
 - Enable broadcast distribution of critical information
 - Achieve faster response and repair time
- b. Applicability to government needs
Since data confidentiality and security are a key aspect of the government entity's communication process, Team on the Run provides a secure and fully controlled environment to the local, state and federal government staff in the office or in the field; allowing them to communicate via smartphones and tablets. See above items to see how Team on the Run capabilities translate into organization benefits.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
US Cellular provides Team on the Run to 30 active customers with over 400 licenses. StreamWIDE has 150+ organizations utilizing Team on the Run SaaS in US with a total of 10,000+ active end users.

Some specific Team on the Run customers:

EMS

Shurmed EMS
Rockwell Medical, Inc
Garden State Medical Transportation
Interborough Developmental and Consultation

Municipalities

City of Oldbridge Township
Downtown Schenectady
Downtown DC
Tampa Downtown

School districts

Vallejo Unified school district
Washington Unified school district
Richmond Public school VA

- d. Overall interoperability of turnkey system for government use
With its key features, 99.999% guaranteed uptime SLA and military-grade secured communication Team on the Run can fulfill any state, local and federal government secure messaging needs.

The solution is deployed on a SaaS/ cloud model and requires:

- Mobile devices Android / iOS with 3G/4G/5G data plan for mobile users
- Desktop with Chrome/Firefox browser for Web administration or Web client

e. Accessories available for turnkey offering

Team on the Run comes works on mobile devices such as smartphones and tablets and PCs. In addition, Team on the Run works with several device and accessory providers such as Samsung, Sonim XP3/XP5, Kyocera providing its services on ruggedized devices, tablets etc.

Team on the Run also has integration with multiple accessories to enhance the push-to-talk service with RSM and emergency buttons.

- Pryme BT-PTT-Z MINI
- Aina wireless RSM – PTT
- Aina wireless button for emergency
- Klein Valor RSM
- Raxon BT-24HC
- Savox SH-01
- Stone Mountain Phoenix
- Savox
- Klein Drift PTT Earpiece
- Klein Triumph 1-Wire

Compatibility matrix of the above accessories with Android and iOS devices can be provided upon request

f. Thoroughness of the vetting process used to select partners

A thorough industry analysis and full RFP process were used to select StreamWIDE as UScellular's solution provider. StreamWIDE has been recognized among the players within the industry being an expert in carrier-grade telecom solutions serving 130+operators, 100M+ End-Users worldwide with live operations in 71 countries / 5 continents.

g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

The solution has been tested in both UScellular and StreamWIDE labs for integration with related US Cellular solutions, such as UScellular provided mobile devices (Android and IOS smartphones, tablets etc.). The solution is in use both internally and deployed with many US Cellular customers.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

a. Pre-installation coordination

Team on the Run installation will be supported by StreamWIDE and UScellular teams. The following are important elements to work before the solution is deployed

- Understand the customer problem

- Define how Team on the Run will contribute to the solution of problem
- Identify use cases and user roles (admin, dispatcher, users)
- Identify the need of accessories
- Gather user phone numbers to configure and device types (Android / iPhone)

UScellular is responsible for device delivery and data service. StreamWIDE is responsible for Team on the Run solution delivery and SaaS service (or on-premise, if applicable).

b. Project coordination

Team on the Run project coordination will be performed by StreamWIDE and UScellular teams. A limited duration trial of the solution can be coordinated with customer if needed. All StreamWIDE project coordination is done remotely for accounts 500 users or less.

c. Installation and Testing process

Based on the identified user list and use cases Team on the Run team will support the initial setup to maximize the value captured by customer:

- Creation of users
- Configuration of user rights and roles
- Activation of devices
- Assistance with implementation questions

d. Client Infrastructure and support assessment process

Our dedicated support team will work with you to understand your infrastructure and assess your support needs. We will create a comprehensive support plan to meet those needs.

e. End user Acceptance process

Once client installation, activation and deployment are complete StreamWIDE will conduct training with the customer team and we will confirm end user acceptance. Customers can reach Team on the Run support for questions or escalation.

f. Approach to maintenance and support

StreamWIDE customers have access to 24/7 email support. The contact button on the client app links you to the support team.

g. Initial and Ongoing Training provided

Team on the Run training is performed by StreamWIDE team product expert and typically delivered remotely. The training is centered on the customer use cases.

Ongoing questions on the product after initial training can be addressed by Team on the Run support team.

h. On-going support and enhancement over the life of the agreement

The Team on the Run Account Manager is responsible for customer satisfaction and the single point of contact for commercial requests such as additional licenses or plan changes.

Team on the Run is an active product and it continuously evolves. Feature enhancements are pushed via the SaaS platform to customers. Our marketing team communicates the enhancements and our support and account managers are ready to answer any questions. Typically, enhancements in existing features are backward compatible so minimum impact is expected on customers already using the functions.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution

Team on the Run standard implementation includes the following services provided by StreamWIDE for a SaaS implementation.

- Team on the Run Implementation services
 - o Initial configuration and creation of users on SaaS solution
 - o Installation support of mobile client app on staff devices
 - o Training session
- Team on the Run SaaS Service
- Team on the Run Support service

Additional consulting services can be ordered as needed.

On-premise implementation services are not quoted in this proposal but are recommended considering the mission critical aspect of public safety organization needs. StreamWIDE can quote on-premise model upon request.

- b. Experience and qualifications of partners and subcontractors
StreamWIDE implementation and support engineers are full time employees and specialize in the Team on the Run product. Internal processes are in place that allow escalation to product and development managers if questions or issues arise.
- c. Description of Additional Integration and Consulting Services provided
Additionally, StreamWIDE can provide consultation services for:
- Special Integration services (API integration with external systems)
 - On-Premise implementation is recommended, can be quoted upon request



StreamWIDE

Security - Internal Policy

Product Document



StreamWIDE Security 1.0

Product Document

Document History:

Version #	Date	Edition cause	Author(s)
1.0	2019-Feb-10	First release	Cosmin CECANAU

Document Approvals:

Version #	Date	Name	Visa
1.0	2019-Feb-10	Cosmin CECANAU	Security Manager

TABLE OF CONTENTS

1. Policy brief & purpose	4
2. Scope	5
3. Policy elements	6
3.1. Confidential data	6
3.2. Protect personal and company devices	6
3.3. Keep emails safe	7
3.4. Manage passwords properly	7
3.5. Transfer data securely	7
3.6. Additional measures	8
3.7. Social media policy	8
3.8. Internet usage policy	9
3.9. Remote employees	9
4. Disciplinary Action	11
4.1. Take security seriously	11



1. Policy brief & purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

It refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	4/11



StreamWIDE Security 1.0

Product Document

2. Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	5/11

3. Policy elements

3.1. Confidential data

Confidential data is secret and valuable.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive customer data.)
- Constitute the backbone of our business, giving us a competitive advantage

Employees will unavoidably receive and handle personal and private information about clients, partners and our company. We want to make sure that this information is well-protected.

Our company most important confidential assets are:

- In-house developed software
- Unpublished financial information
- Data of Customers/Partners/Vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Each employee is obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

3.2. Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only. We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	6/11

When new hires receive company-issued equipment they will receive instructions for:

- *Disk encryption setup*
- *Password management tool setup*
- *Installation of antivirus/ anti-malware software*

They should follow instructions to protect their devices and refer to our *Internal Support Engineers/ Network Engineers* if they have any questions.

3.3. Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Do not open emails when sender is unknown. Even when sender is known, it may be a fake origin (spoofing). In such cases be cautious if the title or content looks unusual for such sender.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they can refer to our *IT Support department*.

3.4. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every three months.

3.5. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our *Internal Support Engineers* for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	7/11

connection.

- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our *IT Specialists/ Network Engineers* need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our *IT Specialists/ Network Engineers* must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Internal Support engineers are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

3.6. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to *HR/ IT Department*.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy (as described in the corresponding chapters below).

Our *Internal Support Engineers/ Network Administrators* will:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company does all the efforts to have all physical and digital shields to protect information.

3.7. Social media policy

Social media refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them.

We allow employees to access their personal accounts at work. But, we expect them to act responsibly and ensure their productivity isn't affected. Using social media excessively while at work can reduce efficiency and concentration. Whether employees are using their accounts for business or personal purposes, they may easily get sidetracked by the vast amount of available content.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	8/11

We advise our employees to:

- Use their common sense. If employees neglect their job duties to spend time on social media, their decline in productivity will show on their performance reviews.
- Ensure others know that personal account or statements don't represent our company. Employees shouldn't state or imply that their personal opinions and content are authorized or endorsed by our company. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
- Avoid sharing intellectual property like trademarks on a personal account without approval. Confidentiality policies and laws always apply.
- Avoid any defamatory, offensive or derogatory content. It may be considered as a violation of our company's anti-harassment policy, if directed towards colleagues, clients or partners.

3.8. Internet usage policy

Our employees are advised to use our company's internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor.

3.9. Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	9/11



StreamWIDE Security 1.0

Product Document

accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our *Internal Support Engineers/ IT Administrators*.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	10/11

4. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary actions up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face Progressive Discipline, even if their behavior hasn't resulted in a security breach.

Our Progressive Discipline policy outlines the steps we will take to address an employee's misconduct.

We recognize that people make mistakes and our employees may not always follow our policies closely. We want to give our employees a chance to correct their behavior when possible and assist them in the process. We also want to ensure that serious offenses are thoroughly investigated and dealt with.

This policy applies to all our employees.

Our disciplinary process has six steps of increasing strictness. These steps are:

- Verbal warning
- Informal meeting with supervisor
- Formal reprimand
- Formal disciplinary meeting
- Penalties
- Termination

4.1. Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.



StreamWIDE Security 1.0



STREAMWIDE Information Security Management System

Product Document



StreamWIDE Security 1.0

Product Document

Document History:

Version #	Date	Edition cause	Author(s)
1.0	2020-Feb-10	First release	Cosmin CECANAU

Document Approvals:

Version #	Date	Name	Visa
1.0	2020-Feb-10	Zakaria NADHIR	CTO

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	2/19



StreamWIDE Security 1.0

Product Document

TABLE OF CONTENTS

1.General view	4
2.Direction	5
3.Scope	6
4.Top Management Leadership and Commitment	7
5.Internal Audit and Employees Continuous Mindset Growth	8
6.Infrastructure Continuous Security	9
7.Software Continuous Security	10
7.1.IDE: IntelliJ IDEA SonarLint	10
7.2.Version Control System: Subversion	11
7.3.Manual Security Check	12
7.3.1.Team Leader Review	12
7.3.2.Dedicated Testing Team	12
7.4.Automated Security Scan	12
7.4.1.Sonar Qube	14
7.4.2.Lint	16
7.4.3.Mobile Security Framework (MobSF)	18

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	3/19



StreamWIDE Security 1.0

Product Document

1. General view

An Information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data.

The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	4/19



StreamWIDE Security 1.0

Product Document

2. Direction

StreamWIDE guidelines and provisions for establishing, implementing, maintaining and continually improving the internal ISMS are following **ISO/IEC 27001:2013** recommendations.

ISO 27001 is a specification for creating an ISMS. It does not mandate specific actions, but includes suggestions for documentation, internal audits, continual improvement, and corrective and preventive action.

StreamWIDE Top Management and Security Team are doing best efforts to follow and adapt the standard recommendations with the goal of keeping our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	5/19



StreamWIDE Security 1.0

Product Document

3. Scope

The document offers a high level overview over the *concrete and provable* actions taken by the Company in order to ensure continuous security improvements

- Top Management Leadership and Commitment
- Internal Audits and Employees Continuous Mindset Growth
- Infrastructure Continuous Security
- Software Continuous Security

External references should be additionally provided:

- [SW_InternalSecurityPolicy](#) - Internal Security Policy document
- [SW_0G_BusinessContinuityPlan](#) - Business Continuity Plan document

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	6/19



4. Top Management Leadership and Commitment

Top Management assume their responsibilities for Information Security/Business Continuity and ensure all required actions are part of company strategy.

Business Continuity Process

The STREAMWIDE Business Continuity Plan aims to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters include all the cases where business is not able to occur under normal conditions.

The main objectives of the plan are:

- Facilitate effective decision-making to ensure that StreamWIDE operations are restored in timely manner in case of service interruption
- Protect essential facilities, equipment, vital records and other assets
- Protect the well-being of StreamWIDE's employees and customers
- Minimize loss of revenue/customers
- Maintain public image and reputation
- Minimize loss of data
- Minimize the critical decisions to be made in a time of crisis
- Identify teams which would need to respond to a crisis

The process is described in [sw_0G_BusinessContinuityPlan](#) document.

Management follow up and review

The main company security objectives are reviewed each week during the official Masterplan Status Meeting with Product Managers.

Additionally, relevant KPIs on [Software Security](#) are sent weekly for management reviews.

Among other information they include the number of vulnerabilities and bugs reported when scanning the code using tools recommended by OWASP.

Security Events Reporting

Since executives are the ones who have the most influence in an organization, Security objectives or Measures for Crisis management are always part of Top Management communication.

Internal Security Policy

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, Top Management has implemented a number of security measures presented by [SW_InternalSecurityPolicy](#).

With this policy, STREAMWIDE ensures that we gather, store and handle data fairly, transparently and with respect towards individual rights.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	7/19



5. Internal Audit and Employees Continuous Mindset Growth

STREAMWIDE Internal security audits are oriented to people awareness, processes, policies and infrastructure hardening.

Software Audit is treated as independent process using automated solutions according to Continuous Security guidelines.

Auditors

Internal audits are performed and coordinated by employees with **important company history and relevant experience in various domains (development, linux administration, team lead, team management)**.

Cosmin CECANAU

Position: Product Manager Installer Team, Manager of Romania Security department, certified for Internal Auditor iso 27001/2013 international recognition

Activity: Coordinates the security department activities based on priorities (implementations, standards appliance, trainings)

Studied: The Faculty of Automatic Control and Computer Science (Polytechnic University of Bucharest);
In StreamWIDE since 2006 ,

Thomas BOUTON

Position: Chief Software Architect / Chief Security Officer

Activity: Coordinates company security activities according to customers needs, creates and validates software architectures.

Studied : Ecole Nationale Supérieure des Télécommunications de Paris
In StreamWIDE since 2001,

Cristian RADU

Position: Product Manager StreamWIDE Messaging System & SmartMS Backend

Activity: Collaborates with the security department bringing concrete lessons learned, real usecases and needs from Messaging Product life history & SmartMS backend new challenges.

Studied: The Faculty of Electronics Telecommunications and Information Technology (Polytechnic University Bucharest);
In StreamWIDE since 2008,

Scheduling

The frequency for Internal auditing a StreamWIDE Subsidiary depends on the activities performed and the number of employees. It is done once or twice per year.

Normally the audit is done on-site. But depending on situation can be done remotely. The audit lasts *3 to 5 days*.

Reporting and Follow Up

The internal Audit is finished by a "conclusions meeting" with the local management. Also an email with conclusions and action plan is sent to the Top Management.

The actions will be followed up weekly as explained in the "Top Management Leadership and Commitment" chapter.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	8/19



6. Infrastructure Continuous Security

Identifying vulnerabilities and gaining visibility into the number of smart devices and their role within the infrastructure can help reduce the risk of a successful cyberattack.

It's important to keep a detailed inventory of all IoTs, constantly check for new security updates that address known vulnerabilities, and maintain them on a segregated network that's completely isolated from other critical systems.

Actions for increasing the security of the company infrastructure are decided during regular audits or during technical workshops.

Some element are listed below, but for confidentiality reasons there are no concrete technical descriptions for the actions taken.

Network Topology

Keeping up-to-date and understanding our own topological structure of the network, physically or logically it is a key requirement for our administrators.

Network segmentation

Network segmentation is a mandatory element for ensuring security.

VPN

VPN solution having high level encryption and Multi Factor Authentication is a mandatory element to ensure safe remote connections.

Firewall

Firewall is one of the cornerstones of any network security strategy so it is mandatory to use a performant solution.

Backup

Ensuring backups gives fast recovery in case of data loss.

Wifi

Wifi Security hardening has also been taken in consideration.

External Scan

External scanning is regularly notifying the administrators about potential flaws of our network.

Intrusion Detection

Intrusion detection systems or traps are offering precious time in preventing a cyberattack.

Secure Communication

Replacing deprecated protocols with latest secure protocols is also a continuous process.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	9/19



StreamWIDE Security 1.0

Product Document

7. Software Continuous Security

StreamWIDE target is to align all proprietary software modules/applications to the newest recommendations regarding Continuous Security.

This chapter explains the process used to ensure Continuous Security for an Android Mobile Application belonging to StreamWIDE software suite.

The rest of **STREAMWIDE** software modules/applications implement **PARTIALLY** this model at this time.

 Code inspection starts from the very first code view due to specialized IDE.

 A popular version control system is used to ensure that all the changes are tracked or can be reverted.

 Manual checking and testing is done by Team Leaders and dedicated Testing Team.

 Automated scan is done by popular and powerful tools on daily, on demand or on commit basis in order to help the team with comprehensive security reports or regressions alerts.

7.1. IDE: IntelliJ IDEA SonarLint

StreamWIDE Android team uses **IntelliJ IDEA with SonarLint plugin** for code development.

IntelliJ IDEA is a Java integrated development environment (IDE) for developing computer software.

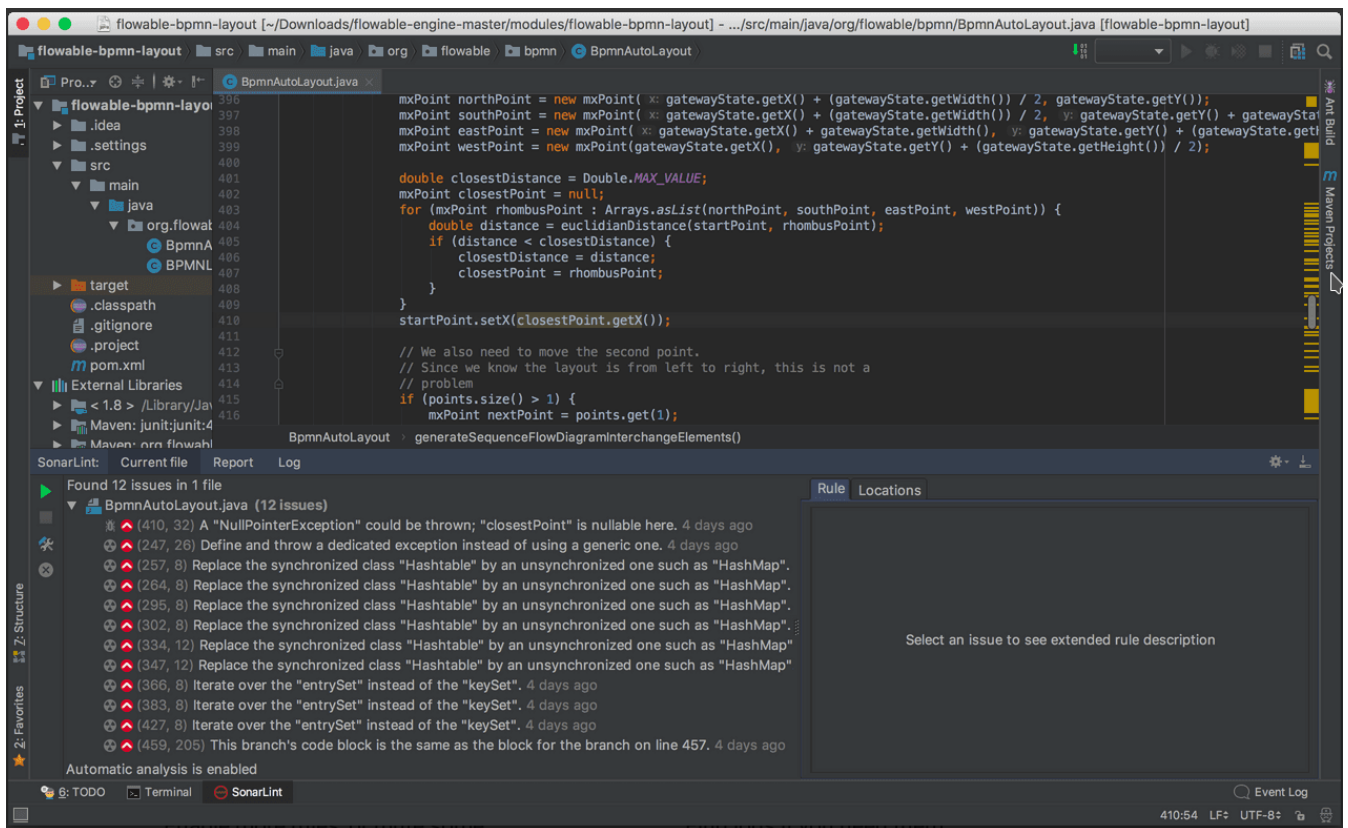
SonarLint is an IDE extension that helps detecting and fixing quality issues as code is being written. Like a spell checker, SonarLint squiggles flaws so that they can be fixed before committing code.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	10/19



StreamWIDE Security 1.0

Product Document



7.2. Version Control System: Subversion

Android Team uses **Subversion** in order to keep the track of every code modification.

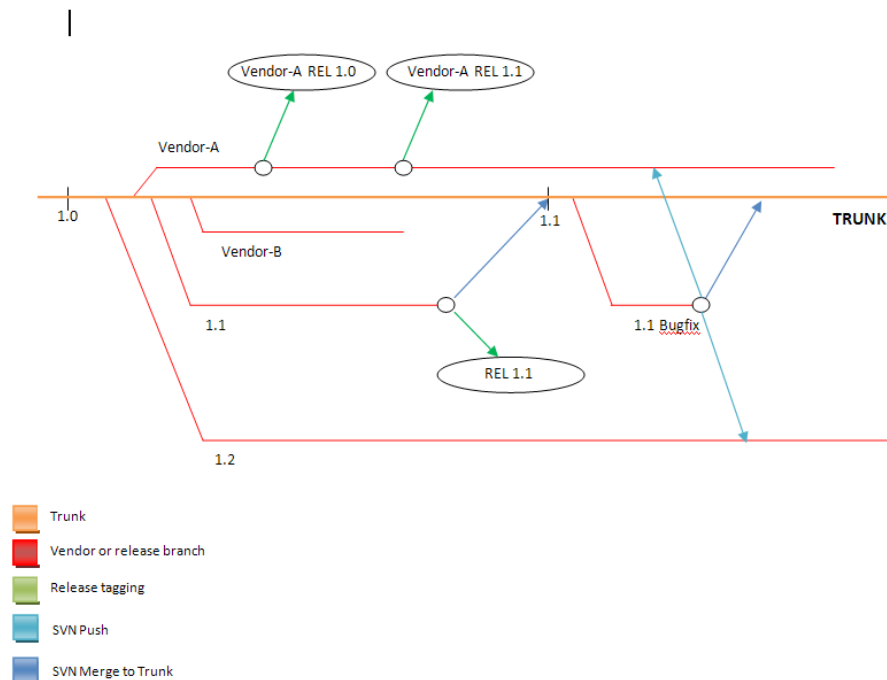


Subversion is a free/open source version control system. That is, Subversion manages files and directories, and the changes made to them, over time.

This allows us to recover older versions of the data or examine the history of how your data changed.

Android Team is using the recommended mechanism with trunk & branches.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	11/19



7.3. Manual Security Check

7.3.1. Team Leader Review

The Android development team distribution ensures a tight control for every piece of code which reaches the repository.

The team is split in small subteams lead by Team Leaders.

Any new code is reviewed by at least a Team Leader before being merged to the main Subversion branch.

Critical code is also reviewed by Product Manager.

7.3.2. Dedicated Testing Team

A dedicated testing team is in-charged of manual testing every new minor and major release.

Although the tests are mostly functional, security fixes receive a special attention and important time allocated.

7.4. Automated Security Scan

A complex mechanism is designed to ensure security scanning on a regular base or on each merge in the main branch (depending on the configuration).

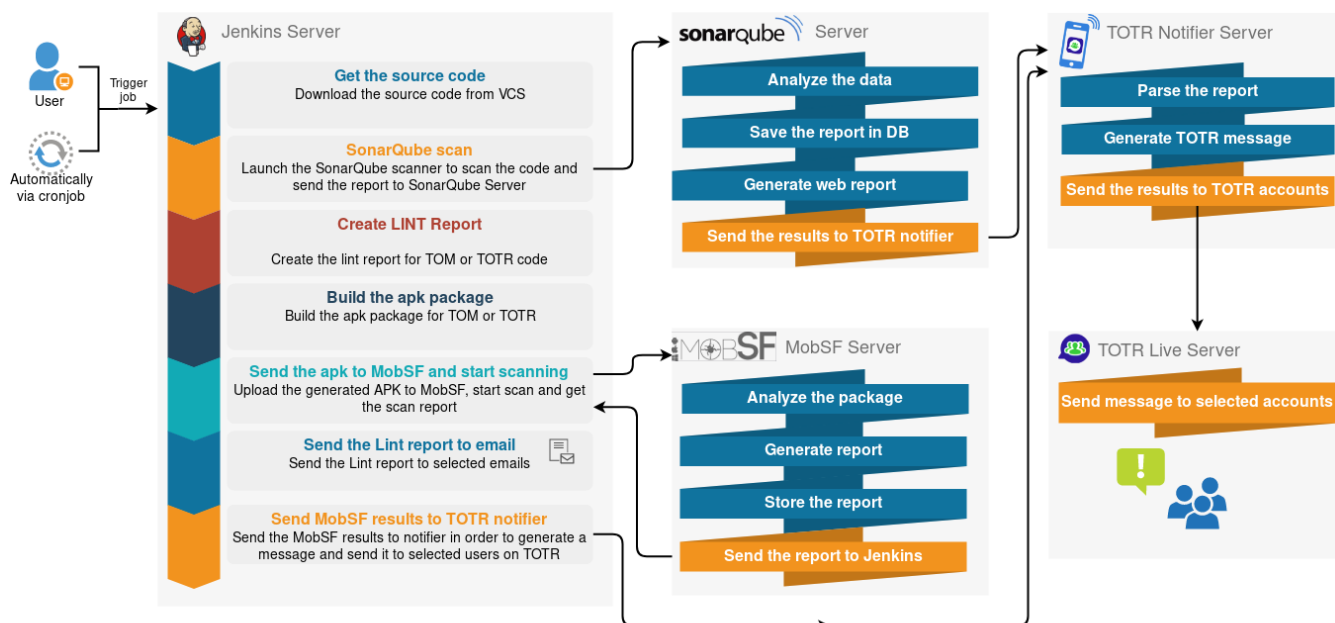
Powerful tools like Jenkins, SonarQube, Lint or MobSF are combined to ensure a complete security verification as it is presented in the diagram below.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	12/19



StreamWIDE Security 1.0

Product Document



© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	13/19

7.4.1. Sonar Qube



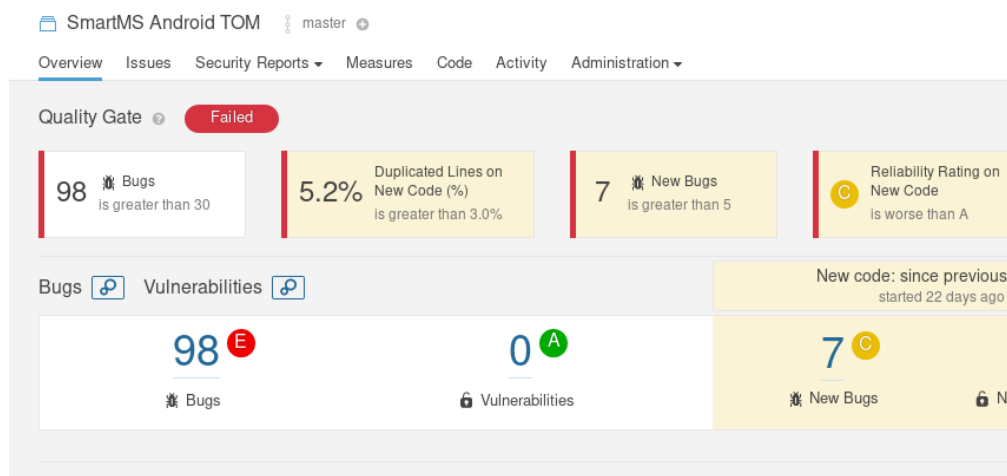
The OWASP SonarQube project aims to provide open source Static Application Security Testing (SAST) using the existing open source solutions.

SonarQube is one of the world's most popular continuous code quality tools and it's actively used by many developers and companies.

SonarQube has helped Android team to improve drastically the quality of the software.

Daily reports are showing the potential vulnerabilities and issues helping the team to understand the threats and principles for good quality and security.

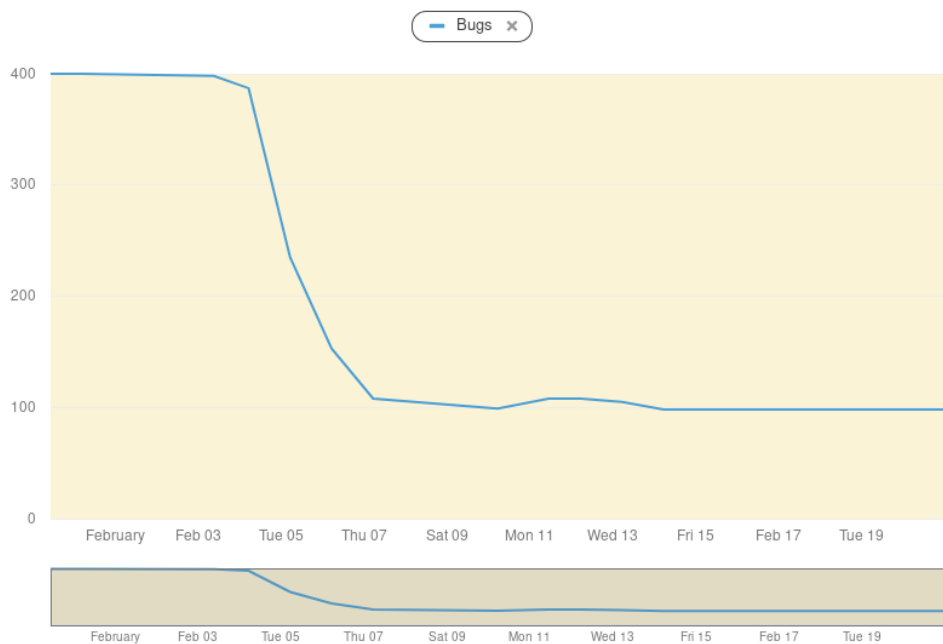
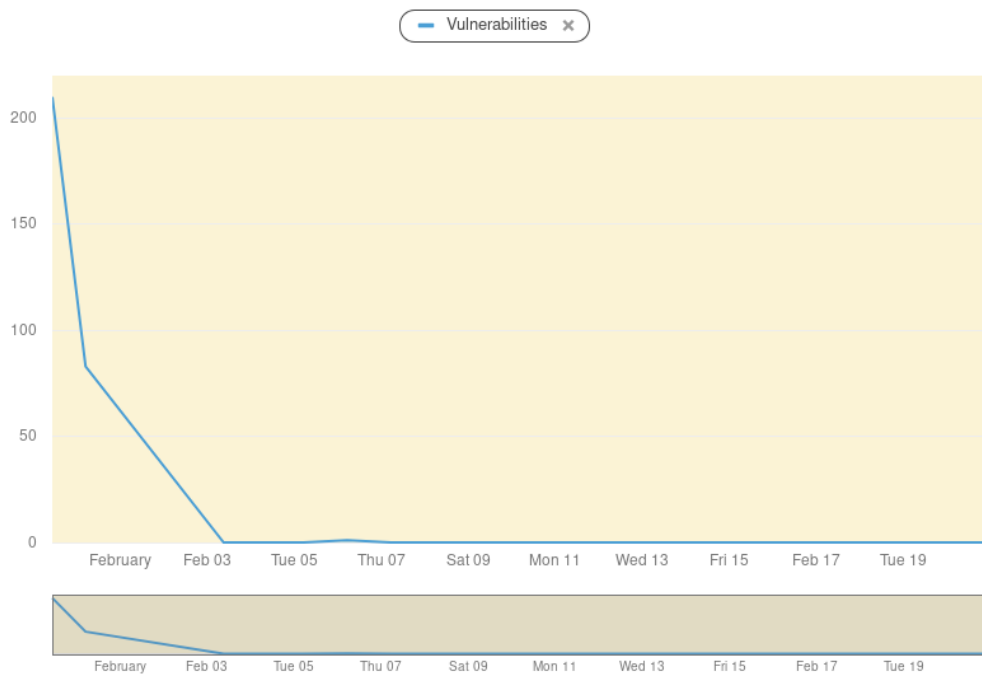
The reports below are taken at 22 Feb 2019. By this date the team has done big efforts to decrease to 0 the number of vulnerabilities and it is concentrating right now to decrease also the number of potential bugs.





StreamWIDE Security 1.0

Product Document



© StreamWIDE All rights reserved	Author: Cosmin CECANAU StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	Date: 2019-Feb-10 15/19



StreamWIDE Security 1.0

Product Document

7.4.2. Lint

Android build system provides a lot of tools to optimize the code, find potential issues, improve performance, etc. One of the tool it supports is Lint. Lint is a tool which analyzes the source code and flags potential bugs and errors during the build.

Daily reports are showing the potential vulnerabilities and issues helping the team to understand the threats and principles for good quality and security.

The reports below are taken at 22 Feb 2019. By this date the team has done big efforts to decrease the number of vulnerability notices and it is concentrating right now to decrease also the number of potential issues..

Overview

Correctness	
4	! MissingRegistered : Missing registered class
9	! ApplySharedPref : Use apply() on SharedPreferences
1	! PrivateApi : Using Private APIs
1	! UnusedAttribute : Attribute unused on older versions
1	! BatteryLife : Battery Life Issues
5	! InflateParams : Layout Inflation without a Parent
1	! NewerVersionAvailable : Newer Library Versions Available
5	! RestrictedApi : Restricted API
54	! SwitchIntDef : Missing @IntDef in Switch
Correctness:Messages	
3	! Typos : Spelling error
Security	
1	! BadHostnameVerifier : Insecure HostnameVerifier
3	! HardwareIds : Hardware Id Usage
1	! SetJavaScriptEnabled : Using setJavaScriptEnabled

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	16/19



StreamWIDE Security 1.0

Product Document

Performance

2	⚠ DrawAllocation : Memory allocations within drawing code
2	⚠ WakelockTimeout : Using wakeLock without timeout
6	⚠ ObsoleteLayoutParam : Obsolete layout params
73	⚠ ObsoleteSdkInt : Obsolete SDK_INT Version Check
3	⚠ StaticFieldLeak : Static Field Leaks
1	⚠ VectorPath : Long vector paths
4	⚠ UseSparseArrays : HashMap can be replaced with SparseArray
1	⚠ DisableBaselineAlignment : Missing baselineAligned attribute
2	⚠ InefficientWeight : Inefficient layout weight
6	⚠ Overdraw : Overdraw: Painting regions more than once
82	⚠ UnusedResources : Unused resources
5	⚠ UselessParent : Useless parent layout
35	⚠ UnusedIds : Unused id
1	⚠ UnusedNamespace : Unused namespace

Usability:Typography

1	⚠ TypographyQuotes : Straight quotes can be replaced with curvy quotes

7.4.3. Mobile Security Framework (MobSF)

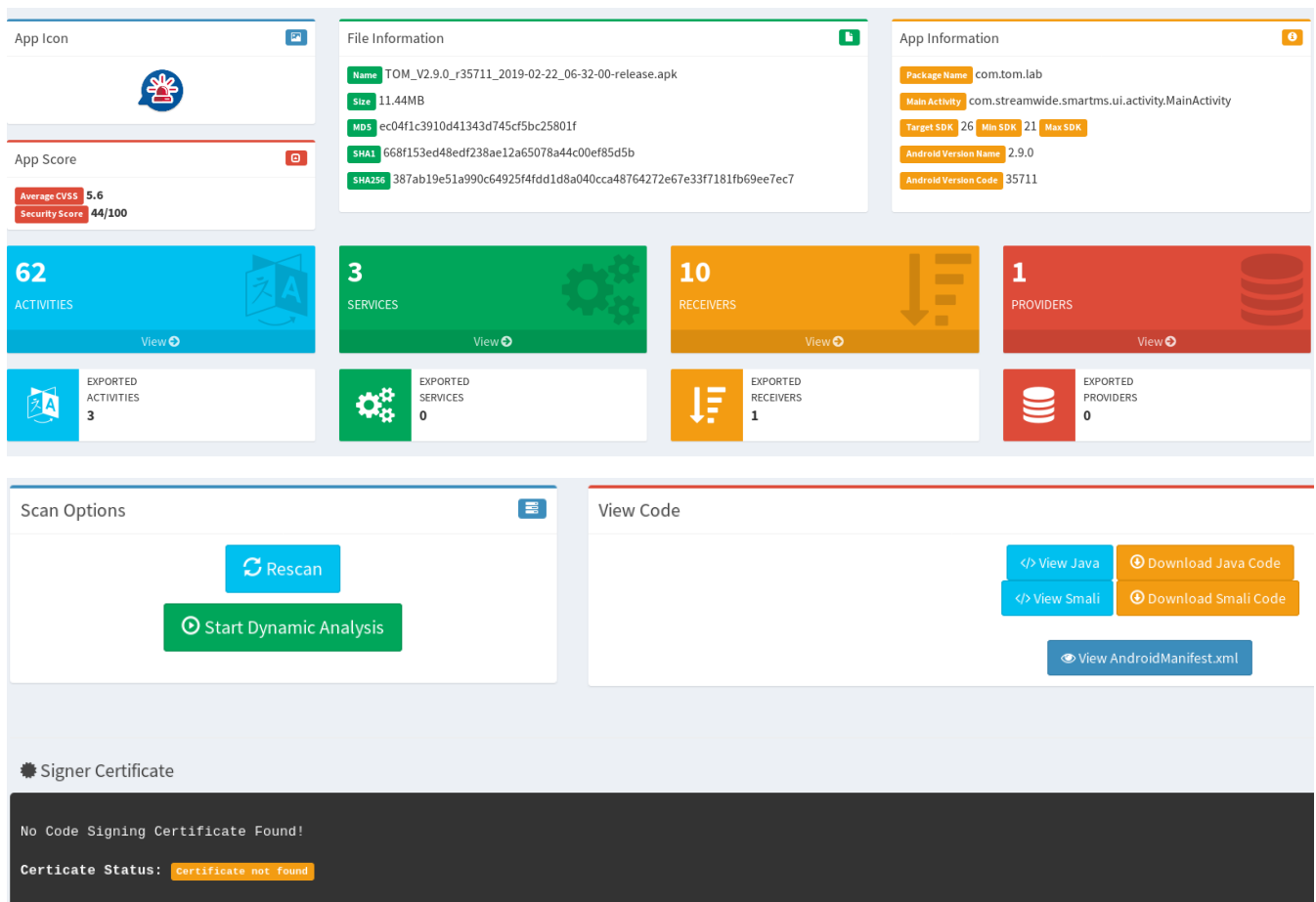


Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing framework capable of performing static, dynamic and malware analysis. It can be used for effective and fast security analysis of Android, iOS and Windows mobile applications and support both binaries (APK, IPA & APPX) and zipped source code.

MobSF can do dynamic application testing at runtime for Android apps.

This option it is used by Android Team on a regular basis to investigate the potential security issues of the apk.

Below are some examples of report taken on 22 Feb 2019.



The screenshot displays the MobSF web interface with the following sections:

- App Icon:** Shows the application icon for 'com.tom.lab'.
- App Score:** Displays an Average CVSS of 5.6 and a Security Score of 44/100.
- File Information:**
 - Name: TOM_V2.9.0_r35711_2019-02-22_06-32-00-release.apk
 - Size: 11.44MB
 - MD5: ec04f1c3910d41343d745cf5bc25801f
 - SHA1: 668f153ed48edf238ae12a65078a44c00ef85d5b
 - SHA256: 387ab19e51a990c64925f4fdd1d8a040cca48764272e67e33f7181fb69ee7ec7
- App Information:**
 - Package Name: com.tom.lab
 - Main Activity: com.streamwide.smartms.ui.activity.MainActivity
 - Target SDK: 26, Min SDK: 21, Max SDK: 28
 - Android Version Name: 2.9.0
 - Android Version Code: 35711
- Summary Metrics:**
 - 62 ACTIVITIES
 - 3 SERVICES
 - 10 RECEIVERS
 - 1 PROVIDERS
- Exported Data:**
 - EXPORTED ACTIVITIES: 3
 - EXPORTED SERVICES: 0
 - EXPORTED RECEIVERS: 1
 - EXPORTED PROVIDERS: 0
- Scan Options:** Includes buttons for 'Rescan' and 'Start Dynamic Analysis'.
- View Code:** Includes buttons for 'View Java', 'Download Java Code', 'View Smali', 'Download Smali Code', and 'View AndroidManifest.xml'.
- Signer Certificate:** Displays 'No Code Signing Certificate Found!' and 'Certificate Status: Certificate not found'.



StreamWIDE Security 1.0

Product Document

Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	dangerous	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and networks.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	19/19



StreamWIDE

Warning Procedure for Internal and External Customers

Operational Guideline

Document History:

Version #	Date	Edition cause	Author(s)
1.0	16/04/2012	First Release	Victorita ANECHITEI

Document Approvals:

Version #	Date	Name	Visa
1.0	16/04/2012	Zakaria NADHIR	ZN

Storage :

PDF Document	Document Sources
Alfresco:\Quality\05.Process&Procedures\Technical Support	Alfresco:\Quality\04.Sources\Technical Support

TABLE OF CONTENTS

1.	Introduction	4
1.1.	Purpose	4
1.2.	Scope	4
1.3.	Definitions and Acronyms	4
1.4.	Role	4
2.	Inputs.....	4
3.	Activities	4
3.1.	On the CTO's side	4
3.1.1.	Gathering and analyzing information	4
3.1.2.	E-mail to Support and Quality	4
3.2.	On the Support Manager's side.....	5
3.2.1.	Warning e-mail internally	5
3.2.1.	Warning e-mail for customers.....	5
3.3.	On the Customer's side	5

1. Introduction

1.1. Purpose

This document describes the policy implemented by StreamWide to insure a proactive support attitude in the case of redundant critical issues and a better circuit of pertinent information inside StreamWide regarding service impacting issues.

1.2. Scope

This procedure relates to the full range of company activities, mainly to issues regarding software development, delivery and technical support.

1.3. Definitions and Acronyms

CTO – Chief Technology Officer

1.4. Role

Under this procedure the CTO is in charge of selecting the pertinent warnings to be sent internally and to the customers.

2. Inputs

Feedback from support, delivery and product teams on critical issues.

3. Activities

3.1. On the CTO's side

3.1.1. Gathering and analyzing information

Every week, the CTO (Zakaria Nadhir) will analyze the main problematic issues that will appear on the customers platforms based on feedback from delivery, support and product teams. He will decide whether there is a real need to send a warning internally and to the customers. The CTO is in charge of selecting the most risky issues among the ones that have been escalated in the given period of time.

3.1.2. E-mail to Support and Quality

As often as needed, the CTO will send an e-mail to the Support and Quality departments to inform them of the main problems that have occurred during the given period and that might risk reappearing on other platforms.

The e-mail sent by the CTO will include for each issue raised:

- a description of the issue

© StreamWIDE	Author: vanechitei	
All rights reserved	sw_OG_Warning Procedure for Internal and External Customers10	4/5

- which are the versions of products that might be impacted
- which are the exceptions to be taken into account when sending the warning e-mails to the customers.

3.2. On the Support Manager's side

3.2.1. Warning e-mail internally

Based on the CTO's e-mail, the support manager must issue a warning e-mail internally with the following list of users, all in Cci:

- support team
- delivery team
- product teams (PMs)
- sales.

Each support engineer has under his direct supervision a list of customers. (See **StreamWIDE Support - Internal Handover Process**, on **Alfreco:\Quality\05.Process&Procedures\Technical Support**). Each of them will have to check in the CRM to see which of his/her customers/platforms might be impacted by the issues raised in the Support Managers' e-mail. If any identified customers, they will inform the Support Manager about it.

This task is considered as level 1 Task, on the support list of tasks.

3.2.1. Warning e-mail for customers

In three days time after having received the CTO's e-mail, the Support Manager will have to send a warning e-mail to all customers concerned by the issues. A special e-mail template will be used for the warning and each customer will receive an individual e-mail (no Cci). Each sent e-mail will be accompanied by the opening of a ticket in the ticketing tool.

- Prior to issuing a warning to customer, Support should inform sales that a warning will be issued. If sales do not answer within 2 workdays, warning is issued, if they ask not to issue or to delay the warning for commercial reasons, they take the responsibility if any problem related to the warning occurs on the platforms. Information to sales should include the solutions they can propose to their customers.
- When the warning is issued to a customer it should contain also a solution/recommendation. A warning with no solution proposed would generate high customer anxiety and may trigger wrong reactions.

3.3. On the Customer's side

Based on the raised issue, the customer should get in touch with his Sales contact inside of StreamWide to be informed of the options that we might propose to fix the issue (e.g. : ask for an upgrade, a fix etc.)

If the customer doesn't reply after two reminders, the Support department is allowed to close the ticket and consider the warning closed.

© StreamWIDE	Author: vanechitei	
All rights reserved	sw_OG_Warning Procedure for Internal and External Customers10	5/5

Appendix Q

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory I: Public Safety

QPP



NASPO

ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
QPP
- b. General Application Area
Subcategory I: Public Safety Systems
- c. General capabilities provided
Wireless QoS, Priority, Pre-emption for 4G Data with private dedicated core network infrastructure.
- d. Expected impact on cost/performance/functionality, etc.
Advanced functionality to ensure prioritized network availability
- e. Subcontractors/partners involved in delivering service
Affirmed, Nokia, Ericsson, Cisco, Palo Alto
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
None from UScellular.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
Data Priority for Public Safety (DPPS) provides public safety agencies and qualifying organizations the ability to have consistent data connectivity when there is heavy network traffic due to a high level of activity at one time.
- b. Applicability to government needs
Quality of Service (QoS) – ensures Public Safety users have access to their mission critical services and applications at the required level of quality when they need it most.

Priority – DPPS customer traffic takes precedence over other traffic on the network.

Preemption – as needed, lower priority traffic is cleared from the network to allow allocation of resources to DPPS users.

Dedicated Core – Network core dedicated to Public Safety; unique SIM.

Fit-for-purpose service – 3 levels of priority to allow for certain users (e.g. Fire/Police Commanders) to be prioritized over other high priority users.

- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
UScellular currently has 1681 business and government customers utilizing the service successfully.
- d. Overall interoperability of turnkey system for government use
UScellular supports a wide range of customization to support interoperability with the infrastructure the government has in place. No interoperability issues have been identified with the solution. Many business and government entities have already implemented the solution without interoperability issues.
- e. Accessories available for turnkey offering
Data Priority (DPPS) SIM cards have been created with a unique color scheme for quick identification, and differentiation from standard SIM cards. These SIM cards enable the Data Priority functionality and must be provisioned for Data Priority services to work properly.
- f. Thoroughness of the vetting process used to select partners
UScellular uses the RFP process to thoroughly evaluate competing vendor solutions against the business needs and objectives. The vendor evaluations include but are not limited to:
 - 1) Alignment with UScellular's system architecture philosophy
 - 2) Availability, reliability, scalability, performance, maintainability, and security requirements
 - 3) Vendor's solution maturity and adoption in North America
 - 4) Vendor's financial standing
 - 5) Standards and Regulatory compliance

The vendor solutions are also trials in a lab prior to being selected.

- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

Lab testing process:

All new components and services provided by the vendor(s) have defined goals captured as use cases. The test cases are defined that trace back to the use cases. To verify and validate that the overall solution achieves its goals without any defects, the test cases are executed against the system in the test lab. The test cases validate the solution both at the component and system integration level. Regression test suite is also executed against the system to verify/validate existing system functionality is free of any new defects. Before going live, a similar verification and validation process is executed in the production environment.

Production ATP (Acceptance Test Plan) process:

For ATP Testing, we have standard test cases for all call flows that a particular network component must pass (based on already deployed services). We then work with our vendor (every SoW we do with our vendors to deploy new elements or services has a section that calls out the ATP creation steps, execution steps and that all tests must pass) and our lab teams (ATS/ASEP/lab personnel) to ensure we incorporate any new test cases for a new service that will be deployed. In order to pass, all regression testing must pass 100% and all new test cases must pass 100%. The ATP is run on both Lab and production sites. We also incorporate failover testing to ensure any new element or service works during both any local or geographical failure, using that same ATP. Each ATP is peer reviewed by multiple engineers and teams.

KPIs (Key Performance Indicators)

KPIs are developed to allow monitoring of key network statistics which would indicate a product or service may not be performing or operating as expected. The KPIs are developed during testing and then subsequently monitored and alarmed on by UScellular's National Network Operations Center (NNOC) throughout the life of the service.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
UScellular's Wireless Solutions Architects perform pre-installation coordination between UScellular and the customer.
- b. Project coordination
A project manager will be assigned as necessary.
- c. Installation and Testing process
Coordinated.
- d. Client Infrastructure and support assessment process
UScellular Wireless Solution Architects with support of Engineering to perform assessments.
- e. End user Acceptance process
No additional end user agreement needed.
- f. Approach to maintenance and support
Dedicated Wireless Solutions Architect.
Dedicated 24x7 National Network Operations Center support.
Specialized Technical Support team to triage customer issues.
Notifications supplied of planned network maintenance (Upgrades, Feature Enhancements) and outages.
- g. Initial and Ongoing Training provided
UScellular offers training to customers at no additional charge.
- h. On-going support and enhancement over the life of the agreement
UScellular continually enhances its network and services to ensure the utmost reliability and availability for its customers. Customer focused support is provided for the life of the contract.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
 - Dedicated Wireless Solutions Architects for the account.
 - Dedicated Technical Customer Service IoT support queue.
 - Dedicated 24x7 emergency support via the National Network Operations Center.
- b. Experience and qualifications of partners and subcontractors
 - As part of our RFP activities, we carefully review the qualifications and capabilities of potential vendors through the information they provide and confirm these qualities/capabilities through reference calls and other available benchmarking data.
- c. Description of Additional Integration and Consulting Services provided
 - Depending on customer's chosen solution, additional consulting and integration services are available.

Appendix R

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory I: Public Safety

Wireless Priority Service (WPS)



NASPO

ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
Wireless Priority Service (WPS)
- b. General Application Area
Subcategory I: Public Safety Systems
- c. General capabilities provided
Wireless Priority Service
- d. Expected impact on cost/performance/functionality, etc.
Advanced functionality to ensure prioritized voice service availability
- e. Subcontractors/partners involved in delivering service
Affirmed, Nokia, Ericsson, Cisco, Palo Alto, Metaswitch
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
None from UScellular. The organization would register with Homeland Security.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
WPS helps ensure the preparedness of the nation to prevent, respond to, and recover from threats, domestic attacks, major disasters, and other emergencies.
- b. Applicability to government needs
WPS provides approved organizations and emergency agencies the ability to place wireless calls when there is heavy network traffic due to a high level of activity at one time. National Security and Emergency Preparedness calls will be queued and given priority treatment to establish continuity of operations and government.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
UScellular currently has 1360 business and government customers utilizing the solution successfully.
- d. Overall interoperability of turnkey system for government use
UScellular supports a wide range of customization to support interoperability with the infrastructure the government has in place. No interoperability issues have been identified with the solution. Many business and government entities have already implemented the solution without interoperability issues.
- e. Accessories available for turnkey offering
None are offered

f. Thoroughness of the vetting process used to select partners

UScellular uses the RFP process to thoroughly evaluate competing vendor solutions against the business needs and objectives. The vendor evaluations include but are not limited to the following:

- 1) Alignment with UScellular's system architecture philosophy
- 2) Availability, reliability, scalability, performance, maintainability, and security requirements
- 3) Vendor's solution maturity and adoption in North America
- 4) Vendor's financial standing
- 5) Standards and Regulatory compliance

The vendor solutions are also lab trialed prior to being selected

g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

Lab testing process:

All new components and services provided by the vendor(s) have defined goals captured as use cases. The test cases are defined that trace back to the use cases. To verify and validate that the overall solution achieves its goals without any defects, the test cases are executed against the system in the test lab. The test cases validate the solution both at the component and system integration level. Regression test suite is also executed against the system to verify/validate existing system functionality is free of any new defects. Before going live, a similar verification and validation process is executed in the production environment.

Production ATP (Acceptance Test Plan) process:

For ATP Testing, we have standard test cases for all call flows that a particular network component must pass (based on already deployed services). We then work with our vendor (every SoW we do with our vendors to deploy new elements or services has a section that calls out the ATP creation steps, execution steps and that all tests must pass) and our lab teams (ATS/ASEP/lab personnel) to ensure we incorporate any new test cases for a new service that will be deployed. In order to pass, all regression testing must pass 100% and all new test cases must pass 100%. The ATP is run on both Lab and production sites. We also incorporate failover testing to ensure any new element or service works during both any local or geographical failure, using that same ATP. Each ATP is peer reviewed by multiple engineers and teams.

KPIs (Key Performance Indicators)

KPIs are developed to allow monitoring of key network statistics which would indicate a product or service may not be performing or operating as expected. The KPIs are developed during testing and then subsequently monitored and alarmed on by UScellular's National Network Operations Center (NNOC) throughout the life of the service.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
UScellular Wireless Solutions Architects perform pre-installation coordination between UScellular and the customer.
- b. Project coordination
A project manager will be assigned as necessary.
- c. Installation and Testing process
Coordinated.
- d. Client Infrastructure and support assessment process
UScellular Wireless Solution Architects with support of Engineering to perform assessments.
- e. End user Acceptance process
Agency will have to initiate a request by going to Department of Homeland Security (WPS)

Agency will have to select the appropriate option before completing the request. Once submitted, the DHS Priority Telecommunications Service Center will contact the customer within five business days to review the request. Supporting documentation may be required.

Once approved, agency will receive website login information (by email) and a GETS card (by U.S. Mail) within 10 business days. Notification of any WPS activations will be sent to the POC via email once the carrier provides enrollment confirmation.

- f. Approach to maintenance and support
Dedicated Wireless Solutions Architect.
Dedicated 24x7 National Network Operations Center support.
Specialized Technical Support team to triage customer issues.
Notifications supplied of planned network maintenance (Upgrades, Feature Enhancements) and outages.
- g. Initial and Ongoing Training provided
UScellular offers training to customers at no additional charge.
- h. On-going support and enhancement over the life of the agreement
UScellular continually enhances its network and services to ensure the utmost reliability and availability for its customers. Customer focused support is provided for the life of the contract.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
 - Dedicated Wireless Solutions Architects for the account.
 - Dedicated Technical Customer Service IoT support queue.
 - Dedicated 24x7 emergency support via the National Network Operations Center.
- b. Experience and qualifications of partners and subcontractors
 - As part of our RFP activities, we carefully review the qualifications and capabilities of potential vendors through the information they provide and confirm these qualities/capabilities through reference calls and other available benchmarking data.
- c. Description of Additional Integration and Consulting Services provided
 - Depending on customer's chosen solution, additional consulting and integration services are available.

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory F: Mobile Data Collection/Mobile Forms

Subcategory I: Public Safety Systems

Subcategory M: Enterprise Messaging

Client Company name:

Tennessee Trash Service Solution

Client name of contact:

Steve Turner

Client contact title:

Owner

Client is a daily user, occasional user, etc.:

Daily

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Kevin Dylla no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

Vendor used: Team On The Run by StreamWIDE

Steve Turner, Owner

Cell: 865-740-7771

stevet@tntrashservice.com

Licenses: 68 Team on The Run licenses

Tennessee Trash Service is a residential & commercial garbage removal company located in Knoxville, Tennessee. We were interested in a new fleet solution for drivers covering a 100-mile radius of Knoxville with different routes every day. We were using push to talk on basic phones to dispatch the entire fleet, which was inefficient, noisy and chaotic by giving verbal turn by turn directions and also trying to determine drivers' locations to pick up misses. Fleet solution would need to refresh data more frequently to have more accurate speed alerts to enforce safety policies. Lastly, we wanted to see all of the routes in the fleet management portal to ensure route optimization.

2. Would you recommend USCC to other customers? Why?

Yes, because the product is easy to use, saves time and saves money.

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

Met milestones

4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?

5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?

Replacing basic driver phones with ruggedized smart phones with Team on the Run for push to talk capability helped making the dispatch process easier & more productive by pushing out Google Map links to drivers for direction, drivers sending pictures/videos from the field, group messaging reducing the chatter in dispatch. MaaS360 locked down the driver smartphones only allowing access to phone calls, Team on the Run, Weather and Google Maps.

6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?

N/A

7. Is there anything else you think we should know about working with USCC or using USCC's products and services?

N/A

8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?

None

Appendix S

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

**Subcategories J and O: IoT Management and Utility
Operations, Monitoring and Support**

LEC iQ2



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
iQ2-Remote Monitoring and Control Industrial IoT Platform.
- b. General Application Area
Subcategories J and O: IoT Management, Utility Operations, Monitoring and Support
- c. General capabilities provided
Remote monitor and control of industrial and municipal assets. Including, but not limited to: Pumps, compressors, generators, water/wastewater infrastructure, utility/energy infrastructure, remote sensors, ITS assets, etc.
- d. Expected impact on cost/performance/functionality, etc.
 - Reduced truck-rolls to remote sites and infrastructure - reduces costs and increases safety
 - Establish state and federal compliance for remote monitoring of disconnected or unmanaged field assets
 - Provide real-time and historical data analytics to improve operational efficiency and reduce related costs
 - Provide alerting and alarming to mission critical assets to reduce risk of system failures and costs associated with such failures
 - The cloud-based application provides real-time insight into asset performance via any web-enabled device or handset decreasing response time to critical field failures.
 - Highly flexible system allows low-cost and simple integration with existing systems.
 - Non-proprietary hardware allows for quick availability and competitive costs on off-the shelf hardware across multiple OEM's.
- e. Subcontractors/partners involved in delivering service
UScellular partners with LEC to provide this solution.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
 - Highly flexible application that easily integrates with existing field assets such as PLC's HMI's and RTU's.
 - Simple configuration process for digital, analog, ethernet and RS485 data types and protocols
 - Remote access capabilities to PLC's and existing infrastructure through the cellular or non-cellular edge gateway
 - User interface fully functional for remote monitoring and control via any web-enabled device.

- No coding or software development in order to integrate most edge assets
 - Speed and simplicity of deployment reduces deployment costs and reduces need for highly technical staffing resources
 - Ongoing support and maintenance do not require professional engineering resources
 - Alerting and alarming functions reduce field failures and provide insight into root cause and needed field support
 - Daily, Weekly and Monthly reporting provide data needed for compliance and granular analytics
- b. Applicability to government needs
This remote monitor and control technology supports a broad application and many different use cases.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
Several hundred sites throughout the US and Canada. References readily available based on application.
- IIoT water/wastewater market*
Ronnie Jones
Aqua Products, Inc
Sarasota, FL 32505
850-469-1133
- d. Overall interoperability of turnkey system for government use
API's can be made available to integrate with other systems in use.
- e. Accessories available for turnkey offering
- Cellular communication gateways
 - UL 508A Certified IoT-Ready Panels-Gateway, I/O, Power Supply, UPS backup, antenna, wiring, in all in a ready-to-deploy enclosure
 - Cellular antennas and cable
 - HMI's, PLC's and other automation hardware
 - Professional Services-Engineering and Integration
- f. Thoroughness of the vetting process used to select partners
We do not use partners for this application. Should installs be required as part of a turnkey solution, third-party recommendations can be provided.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
Full Factory Acceptance Test (FAT) completed and documented prior to shipment/deployment.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package. The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination

Site Survey and Solution Discovery planning is completed by the assigned Project Manager through collaboration with client. Site Survey Document is completed and fully documented based on project needs. Site Survey is provided to customer for final acceptance and approval. Automation requirements are developed and reviewed with client and formal customer sign-off completed upon acceptance of any control narrative.

b. Project coordination

LEC Project Management and Engineering Resources are assigned based on application/solution type and needs. Project management stays engaged throughout every stage of the process. Depending on project scope, reoccurring team calls are scheduled to meet project demands, timelines and expectations with Project Reports provided on a consistent basis.

c. Installation and Testing process

Pilots are a common process in order to optimize the solution requirements and deployment model. Pre-Install testing is completed through FAT testing at LEC facilities prior to shipment, installation, and deployment. Installation is typically customer driven due to simplicity of install or utilizing existing 3rd party municipal vendor. All installation instructions and wiring diagrams are provided with real-time support during field installation and final functional testing.

d. Client Infrastructure and support assessment process

LEC provides infrastructure and assessment through the site-survey and then finalized during the completion of the quality assessment process.

e. End user Acceptance process

- Completion of LEC iQ2 Quality Assurance Process Document
- 30, 60, and 90 Day QA customer engagement process
- Solution Training/Refinement process
- SolveIT Support Tool training
- Final customer sign-off at 90 days

f. Approach to maintenance and support

- 24/7/365 Access to SolveIT support ticketing system is standard
- Advanced notices of system maintenance and upgrades provided
- iQ2 Feature and Functionality upgrade notices provided
- Standard Support Services as provided in iQ2 Services Agreement
- Extended Support Services available

g. Initial and Ongoing Training provided

- iQ2 User and Admin Training prior to deployment
- 30, 60, and 90-day Training Program as part of the iQ2 Quality Assurance process
- Training for iQ2 feature additions provided upon request
- End user and Admin Video Training series available to all LEC Customers

h. On-going support and enhancement over the life of the agreement

See Attached LEC iQ2 Services Agreement

4 - Service Factors:

a. Description of related services included in Turnkey Solution

LEC Turnkey Solutions include:

- Customer Site Survey Support
- IIoT Communications Hardware-From list of iQ2-Ready UL 508A Certified devices
- Delivery of all related wiring and installation diagrams
- Installation support
- Private Cellular Network Connectivity
- Site Engineering Support Admin and User Access to the iQ2 Remote Monitoring and Control Platform
- 24/7/364 Access to SolveIT Support Tool

b. Experience and qualifications of partners and subcontractors

LEC does not utilize partners or subcontractors on a standard deployment.

c. Description of Additional Integration and Consulting Services provided

- Site Survey Support Services
- IIoT Engineering Support Services
- Network Engineering Services
- LEC Installation Services

We have a full Products and Services guide that is available upon request.

EXHIBIT D

SUPPLIER TERMS AND CONDITIONS

iQPulse™ TERMS AND CONDITIONS AGREEMENT

YOU MUST READ THIS iQPulse™ TERMS AND CONDITIONS AGREEMENT CAREFULLY. THE SERVICE IS PROVIDED TO THE CUSTOMER SUBJECT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT.

Section 1. Definitions.

1.1 "Agreement" means this iQPulse™ Terms and Conditions Agreement, as may be amended from time to time in accordance with the terms and conditions hereof.

1.2 "Communication Facility(ies)" means any wired or wireless instrumentality or service (or any combination thereof) used as a pathway for enabling Customer's use of the Service, including the Internet.

1.3 "Company" means LEC, Inc., a Mississippi business corporation, having its principal offices located at 110 Excell Drive Pearl, Mississippi 39208, together with each entity that it directly or indirectly owns or controls.

1.4 "Components" means the individual modules, features or products that make up the System. From time to time, new Components may be introduced, and access to those Components may be restricted depending on the terms of the particular Service.

1.5 "Connectivity Agreement" means the agreement between USCC and Customer governing Customer's subscription to any Communication Facility(ies) provided by USCC in connection with the Service.

1.6 "Customer" means the individual or entity who is a subscriber to any Communication Facility(ies) provided by USCC in connection with the Service.

1.7 "Customer Data" means any of Customer's information, documents, or electronic files that are either (A) transmitted through an Endpoint in connection with the Service, or (B) provided to Company hereunder for any purpose. At all times Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, security, appropriateness, ownership and permanent storage and safekeeping of all Customer Data.

1.8 "Effective Date" means the date of Customer's acceptance of this Agreement.

1.9 "Emergency System Maintenance" means any extraordinary, unscheduled maintenance to the System (or its Components) performed by Company for the purpose of immediately addressing any issue that affects the security or availability of the System.

1.10 "Endpoint(s)" means any iQPulse™ enabled device, or other device or asset generating Customer Data that is populated into the System.

1.11 "Event(s) of Default" means Customer's failure to perform or observe any other term, condition, or covenant to be performed by it under this Agreement.

1.12 "Force Majeure Event" means any (A) act(s) of war, hostility, or sabotage, including denial of service attacks; (B) act(s) of God; (C) electrical, Internet telecommunication outage or security breach that is not caused by the obligated Party; (D) government restrictions (including the denial or cancellation of any export or other license); and/or (E) any other event outside the reasonable control of the obligated Party.

1.13 "Notice" means any notice(s), consent(s), communication(s) and exchanges of information between the Parties as may be required hereunder. All Notices shall be provided in writing and shall be delivered personally, by registered or certified letter (return receipt requested), by courier or facsimile, and unless otherwise provided for in this Agreement shall be deemed effectively served (A) if by personal delivery, immediately upon such delivery; (B) if by registered or certified mail, five (5) calendar days after mailing; (C) if by courier, three (3) days after deposit; and (D) if by facsimile, immediately upon dispatch if receipt is confirmed electronically. All Notices shall be sent to the appropriate receiving Party's addresses as follows (or such other address as may have been furnished by or on behalf of such Party by like Notice): (i) if to Company – LEC, Inc., Post Office Box 127, Brandon, Mississippi 39043-0127; and (ii) if to Customer – the address identified as Customer's address in the Connectivity Agreement.

1.14 "Party" means Company or Customer, and every reference to a Party includes its successors and permitted assigns; and "Parties" means, collectively, Company and Customer and their respective successors and permitted assigns.

1.15 "Regular System Maintenance" means any regular, scheduled maintenance to the System (or its Components) performed by Company for the purpose of improving the functionality or security of the System.

1.16 "Service" means access to the System and its Components, together with certain additional related services, which depending upon the particular Service used by Customer may or may not include (A) temporary storage or backup of Customer Data; (B) hosting of Customer remote-site web pages(s); (C) remote troubleshooting (to the extent it relates to an embedded System device client application); (D) user-access management; (E) Customer support services; and (F) any other related services that Company may make available from time to time. Expressly excluded from the definition of Service are any and all Communication Facilities provided by Customer and/or any Third Party with whom Customer has an agreement to provide Communication Facilities.

1.17 "System" means the iQPulse™ platform, including any updates and improvements relating thereto and any derivative works of the foregoing. The System is made up of individual Components.

1.18 "Third Party" means any person or entity that is not a Party to this Agreement.

1.19 "USCC" means USCC Services, LLC, a Delaware limited liability company, having its principal offices located at 8410 W. Bryn Mawr, Chicago, Illinois 60631, together with each entity that its parent company United States Cellular Corporation directly or indirectly owns or controls. USCC is acting as a reseller of the Service.

Section 2. Rights and Restrictions of Use of the Service.

2.1 Customer Use Rights. During the Term hereof (as hereinafter defined) and subject to the terms and conditions of this Agreement, Company hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable right to connect the Endpoints to the Service for Customer's business purposes. The use right in the preceding sentence is strictly limited to the number of Endpoints as identified in the Connectivity Agreement. Said use rights are non-transferable, except in the event of a voluntary transfer of substantially all assets by Customer to a transferee which executes Company's form of agreement agreeing to be bound by all of the terms and conditions of this Agreement. All rights in and to the use of the Service not expressly granted to Customer herein are reserved to Company, and Customer agrees that Customer does not acquire any rights to use the Service in excess of the scope and/or duration of the term of this Agreement; provided, however, that Customer shall retain all ownership and intellectual property rights in and to the Customer Data. The rights of Customer to use the Service on a particular Endpoint cannot be shared or used by, on or for more than one Endpoint. To the extent that it may be appropriate or necessary in any particular Customer application to utilize any Third Party hardware,

software or technology with the Service, Customer's right to use such Third Party hardware, software or technology shall be governed by the terms of the applicable Third Party hardware, software or technology license agreement and not under this Agreement. To the extent that the Service may enable Customer to add links to web sites and access to content, products and services of any third parties (including users, advertisers, affiliates and sponsors of such third parties), Company is not responsible for any such Third Party web sites or Third Party content provided on or through the Service and Customer assumes and shall bear any and all risks associated with the access and use of such web sites and Third Party content, products and services. Upon the expiration or earlier termination of this Agreement as provided herein, all rights of Customer to use the Service shall terminate.

2.2 Availability of Service. At all times during the Term hereof, Company warrants that Company will provide to Customer access to the Service on a twenty-four (24) hours, seven (7) days per week basis at an availability rate of at least ninety-nine point nine percent (99.9%) (the "Service Uptime"). Service Uptime shall be calculated to the nearest minute occurring during each calendar month of the Term and shall be continuously monitored through Company's automated systems.

2.3 System Maintenance. Company may perform Regular System Maintenance on an as-needed basis (typically occurring between the hours of 9:00 P.M. and 4:00 A.M. Pacific Time), which in certain circumstances may result in an interruption of Service Uptime. Company will provide to Customer a minimum of fifteen (15) days advance Notice of any Regular System Maintenance to be conducted, and in circumstances where an interruption in Service Uptime is expected to occur shall specify in said Notice the anticipated duration of such interruption. In unexpected circumstances where Company is required to perform Emergency System Maintenance, Company will provide to Customer advance Notice of any Emergency System Maintenance as reasonably possible under the circumstances.

2.4 Storage and Backup of Customer Data. In the event that the Service subscribed to by Customer includes the temporary storage or backup of Customer Data (as applicable), Company will temporarily store or backup any Customer Data populated to the System (or portion thereof as may be designated by Customer) up to a maximum of either (A) a period of twelve (12) months, or (B) a limit of five hundred thousand (500,000) database records, whichever occurs first; provided, however, that the foregoing database record limit may be affected by the configuration of the device(s) comprising each Endpoint and/or the specific data value update rates determined by Customer's use of the Service.

2.5 Customer Support. Company agrees to provide normal Customer support on weekdays between the hours of 8:00 A.M. and 5:00 P.M. Central Time, during which time Company will respond to a request for Customer support within one (1) hour or less. Further, Company agrees to provide after-hours Customer support on weekdays between the hours of 5:00 P.M. and 8:00 A.M. Central Time and on weekends via Company's solveIT® ticketing system, during which time Company will respond to a request for Customer support no later than 10:00 A.M. Eastern Time the following business day.

2.6 Company Use Rights. During the Term and subject to the terms and conditions of this Agreement, Customer hereby grants to Company a non-exclusive, non-transferable, non-sublicensable right to use, copy, transmit, store, modify and display the Customer Data solely for purposes of Customer's use of the Service; otherwise, Company shall not use the Customer Data except to improve the Service and/or as necessary to perform its obligations hereunder. Company may compile statistical information related to the performance of the Service, and at its election make such information publicly available, provided that such information does not incorporate Customer's identify, any Customer Data, and/or any of Customer's Confidential Information (as hereinafter defined), and Company shall retain all intellectual property rights in and to such information.

2.7 Customer Use Restrictions. At all times during the Term hereof, Customer expressly covenants and agrees not to use or permit use of the Service, including without limitation by uploading, emailing, posting, publishing or otherwise transmitting any Customer Data or other material, for any purpose that may (A) menace or harass any person or cause damage or injury to any person or property; (B) involve

the publication of any material that is false, defamatory, harassing or obscene; (C) violate privacy rights or promote bigotry, racism, hatred or harm; (D) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (E) constitute an infringement of intellectual property or other proprietary rights of any Third Party; or (F) otherwise violate applicable laws, ordinances or regulations. In addition to any other rights afforded to Company hereunder, Company expressly reserves the right to suspend access to the Service for any violation of the foregoing restrictions and shall have no liability to Customer in the event that such action is taken. Customer expressly acknowledges that the Service is not intended for use with protected health information under HIPAA, credit card numbers, financial account numbers, or other similarly-sensitive personal information, and that Customer assumes all risk arising from use of any such sensitive information with the Service, including the risk of any inadvertent disclosure or unauthorized access thereto. Customer is responsible for ensuring that Customer's use of the Service is in compliance with all applicable laws and governmental regulations (including without limitation those set forth in Section 7 of this Agreement), and Customer acknowledges that Customer assumes all risk arising from any such use that is not compliant with applicable laws and regulations.

2.8 Other Restrictions. In addition to those restrictions set forth in Section 2 hereof, with respect to either the Service and/or the System, as applicable, Customer shall not, directly, indirectly, alone, or with another party either (A) remove or modify any Company markings or any statement or declaration of Company's proprietary rights; copy, disassemble, reverse engineer, or decompile the System; (B) modify, create derivative works based upon, or translate the System; (C) license, sell, rent, lease, transfer, grant any rights in or otherwise commercially exploit the Service in any form to any other party; (D) access or use the Service in order to build or support, and/or assist a Third Party in building or supporting, products or services competitive to Company; (E) other than the Customer Data, disclose the results of the Service without Company's prior written consent; or (F) attempt to do any of the foregoing or cause or permit any Third Party to do or attempt to do any of the foregoing. At all times Company shall own all right, title and interest in and to any and all intellectual property rights (including all derivatives or improvements thereof) in the Service, and any suggestions, enhancement requests, feedback, recommendations or other information provided by Customer relating to the Service.

3. Non-Disclosure of Confidential Information. By virtue of this Agreement, the Parties may have access to one-another's information that the owning Party considers confidential in nature (the "Confidential Information"). Accordingly, each Party expressly covenants and agrees to disclose only information that is required for the performance of their respective obligations under this Agreement. The term "Confidential Information" shall also include the terms under this Agreement, any Customer Data residing in the System environment, and all information clearly identified as confidential at the time of its disclosure. However, a Party's Confidential Information shall not include information that: (A) is or becomes a part of the public domain through no act or omission of the other Party; (B) was in the other Party's lawful possession prior to the disclosure and had not been obtained by the other Party either directly or indirectly from the disclosing Party; (C) is lawfully disclosed to the other Party by a Third Party without restriction on the disclosure; or (D) is independently developed by the other Party. Each Party agrees to hold one another's Confidential Information in confidence for a period of three (3) years subsequent to the expiration or termination of this Agreement, and further agrees to disclose Confidential Information only to its employees or agents who are required to protect it against unauthorized disclosure in a manner no less protective than under this Agreement, and in any event only for the purpose of performing a Party's obligations hereunder. Nothing shall prevent either Party from disclosing the terms under this Agreement in any legal proceeding arising from or in connection with this Agreement or from disclosing the Confidential Information to a governmental entity as may be required by applicable law.

Section 4. Term and Termination.

4.1 Term. The term of this Agreement (the "Term") commences on the Effective Date and remains in effect for the duration of the term of the Connectivity Agreement. The Term will automatically terminate upon the termination or expiration of the Connectivity Agreement. For a period of up to thirty (30)

days subsequent to the effective date of the expiration or termination of this Agreement, upon receipt of written request Company may permit Customer to access the Service solely to the extent necessary for Customer to retrieve any Customer Data to the extent that any such Customer Data resides in the System environment; provided, however, that Customer expressly acknowledges and agrees that Company has no obligation to retain any Customer Data and that any Customer Data residing in the System environment may be irretrievably deleted at any time after thirty (30) days subsequent to the expiration or termination of this Agreement.

4.2 Termination of Service. The Service may be terminated by Company upon the occurrence of an Event of Default by Customer if such Event of Default is not cured by Customer within thirty (30) days subsequent to receipt of a Notice of the Event of Default; provided, however, that in any case of any violation by Customer of Section 2 of this Agreement, the Service may be terminated immediately by the Company.

Section 5. Warranty Disclaimer and Liability.

5.1 Warranty Disclaimer. AS COMPANY DOES NOT CONTROL THE TRANSFER OF DATA OVER OR THROUGH ANY COMMUNICATION FACILITIES, CUSTOMER EXPRESSLY ACKNOWLEDGES AND AGREES THAT (A) COMPANY DOES NOT GUARANTEE THAT THE SERVICE WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT COMPANY WILL BE ABLE TO CORRECT ALL SERVICE ERRORS; (B) THE SERVICE MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATION FACILITIES; AND (C) COMPANY IS NOT RESPONSIBLE FOR ANY ERRORS, DELAYS, DELIVERY FAILURES, OR OTHER DAMAGES THAT MAY RESULTING FROM SUCH PROBLEMS. TO THE EXTENT NOT PROHIBITED BY LAW, EXCEPT AS OTHERWISE PROVIDED HEREIN THERE ARE NO EXPRESS OR IMPLIED WARRANTIES FOR OR CONDITIONS TO THE SERVICE HEREUNDER, INCLUDING COMPATIBILITY OF THE SERVICE WITH ANY SPECIFIC HARDWARE, SYSTEMS, COMMUNICATION FACILITIES, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

5.2 Liability Disclaimer. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF ANY CUSTOMER DATA, REVENUE OR PROFITS (EXCLUDING FEES PAYABLE BY CUSTOMER TO COMPANY UNDER THIS AGREEMENT). COMPANY'S MAXIMUM LIABILITY TO CUSTOMER FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNTS ACTUALLY PAID BY CUSTOMER TO USCC (AS RESELLER) FOR THE SERVICE THAT IS THE SUBJECT OF THE CLAIM IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM

6. Indemnification. In the event that any Third Party should make a claim against either Customer or Company (the "Recipient," which may refer to either Customer or Company depending upon which Party receives the Material), that any information, design, specification, instruction, software, service, data, or material (collectively the "Material") furnished by either Customer or Company (the "Provider," which may refer to either Customer or Company depending on which Party provides the Material), and used by the Recipient infringes on such Third Party's intellectual property rights, the Provider, at its sole cost and expense, shall defend the Recipient against the claim and indemnify the Recipient from any damages, liabilities, costs and expenses awarded by a court of competent to the Third Party claiming infringement or the settlement agreed to by the Provider, provided that the Recipient does all of the following: (A) promptly notifies the Provider in writing, but in no event later than thirty (30) days subsequent to when the Recipient receives Notice of the claim (or sooner if required by applicable law); (B) gives the Provider sole control of the defense and any settlement negotiations; and (C) gives the Provider the information, authority, and assistance the Provider needs to defend against or settle the claim. In the event the Provider believes or it is determined that any of the Material may have violated a Third Party's intellectual property rights, the

Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for its continued use, or in the event that these alternatives are not commercially reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such return materially affects Company's ability to meet its obligations hereunder, then Company may, at its option and upon providing thirty (30) days prior written Notice to Customer, terminate this Agreement. The Provider will not indemnify the Recipient if the Recipient alters the Material or uses it outside the scope of use identified in the Provider's user documentation or services policies or if the Recipient uses a version of the Materials which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was provided to the Recipient. The Provider will not indemnify the Recipient to the extent that an infringement claim is based upon (i) any information, design, specification, instruction, software, data, or material not furnished by the Provider, or (ii) any Material from a Third Party portal or other external source that is accessible to Customer within or from the Service (e.g., a Third Party web page accessed via a hyperlink). Notwithstanding any of the foregoing, Company has no obligation to indemnify Customer in any circumstance where (a) any infringement claim is based upon the combination of any Material with any products or services not provided by Company; (b) any infringement is caused by the actions of Customer against any Third Party if the Service as delivered to Customer and used in accordance with the terms of this Agreement would not otherwise infringe any Third Party intellectual property rights; or (c) any infringement claim is based on (1) a patent that Customer was made aware of prior to the Effective Date of this Agreement (pursuant to a claim, demand, or Notice), or (2) any of Customer's actions occurring prior to the Effective Date of this Agreement. It is the express intent of the Parties that this Section 6 provides each Party's exclusive remedy for any infringement claims or damages.

7. Compliance with Export Laws. The export laws and regulations of the United States as well as other relevant local export laws and regulations may apply to the Service. Customer expressly acknowledges and agrees that (A) to the extent applicable, such export control laws may govern Customer's use of the Service under this Agreement; (B) Customer shall comply with all such applicable export laws and regulations; (C) no data, information, software programs and/or materials resulting from Service (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

8. Force Majeure. Neither Party shall be responsible for any failure or delay in the performance of their respective obligations hereunder provided such failure or delay is caused by a Force Majeure Event; provided, however, that each Party expressly covenants and agrees to use reasonable efforts to mitigate the effect of a Force Majeure Event that should occur during the Term of this Agreement. In the event that a Force Majeure Event occurs and continues for more than thirty (30) days, either Party may cancel any unperformed service upon providing advance written Notice to the other Party.

9. Other Provisions. Time is of the essence of each of the provisions of this Agreement. Customer shall not assign, transfer or encumber this Agreement without obtaining prior written consent of Company, nor shall any attempted assignment, transfer or encumbrance of this Agreement be effectuated by operation of law or otherwise without the prior written consent of Company. Company may assign or transfer this Agreement to any affiliate without obtaining consent from Customer, written or otherwise, and such assignment or transfer shall be effective immediately upon execution and delivery by Company. The Parties hereto expressly acknowledge and agree that, as between the Parties, (A) except as otherwise expressly set forth herein, no representation(s) has been made with respect to the subject matter of this Agreement, nor any representations inducing the execution and delivery of this Agreement; (B) each Party has relied on such Party's own judgment in entering into this Agreement; and (C) any statements and/or representations that may have been made previously by either of them to the other are void and of no effect, and that neither of them has relied upon such statements and/or representations in connection with such Party's dealings with the other. The Parties expressly agree that it is their intention and covenant that

(i) this Agreement constitutes the entire agreement between the Parties regarding the subject matter hereof, and that any and all prior agreements, proposals or communications (whether oral or written) between the Parties are superseded by and merged into this Agreement; (ii) this Agreement, any performance under this Agreement, and all suits and proceedings arising out of, related to, in connection with or by reason of this Agreement between the Parties, be construed in accordance with, and under and pursuant to, the laws of the State of Mississippi; (iii) the laws of the State of Mississippi will be applicable and will govern any action or other proceeding that may be brought by either Party arising out of, related to, in connection with or by reason of this Agreement, to the exclusion of the law of any other forum; (iv) unless expressly waived by Company, the exclusive jurisdiction and venue of any legal action between the Parties with respect to the subject matter of this Agreement shall be the appropriate court(s) in the Southern District of Mississippi; and (v) each of the Parties hereto submits itself to the exclusive jurisdiction and venue of such court(s) for the purpose of any such legal action. If it becomes necessary for any Party to undertake any litigation or to employ an attorney to assist such Party in pursuit of or protection of its rights under this Agreement, the non-prevailing Party shall be obligated to reimburse the prevailing Party for such fees and related costs and expenses, including reasonable attorney's fees, whether incurred at trial, on appeal, or otherwise. The invalidity, illegality, or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if such invalid, illegal, or unenforceable provision had been omitted. This Agreement may be modified or amended by Company from time to time, and where material modifications or amendments are made Company will provide appropriate notice to Customer in such circumstances, whereupon Customer's continued use of the Service will constitute and express acceptance of such modifications or amendments. All terms and conditions of this Agreement shall be binding upon the successors and assigns of the Parties hereto. No waiver of any provision of this Agreement shall be implied by any failure of either Party to enforce any remedy upon the violation of such provision, even if such violation is continued or repeated subsequently. No express waiver shall affect any provision other than the one specified in such waiver, and that only for the time and in the manner specifically stated. Captions to and headings of the Sections and paragraphs of this Agreement are solely for the convenience of the Parties and shall not be used for the interpretation or determination of the validity of the Agreement and/or any provision(s) hereof. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine, neuter, singular or plural as the identity of the person or persons may require. Provisions that survive expiration or termination of this Agreement are those provisions relating to limitation of liability, infringement indemnity and any others which by their nature are intended to survive.

4820-4721-4247, v. 1



iQ2® / iQCommSentry®
WIRELESS SERVICE AGREEMENT No. _____

EXHIBIT "A" (V1) xx/xx/20xx

Business Name
Address
City State Zip
Telephone
Email

Effective Date:

Agreement Term:

Node Summary:

Site	Information

Monthly Charges:

Description	Quantity	Unit Price	Extension

SPECIAL PROVISIONS:

iQ2® / iQCommSentry® WIRELESS SERVICE AGREEMENT

THIS iQ2® / iQCommSentry® WIRELESS SERVICE AGREEMENT (the "Agreement") is made and entered into by and between LEC, INC., a Mississippi Business Corporation (the "Company") and _____, (the "Customer"). Company and Customer may hereinafter be referred to as a "Party" in the singular and the "Parties" collectively.

Section 1. Definitions.

1.1 "Affiliate" of a Party means any entity that controls, is controlled by, or is under common control with, such Party.

1.2 "Acceptable Application" means a software program, application or platform that will be combined with the Service and used by Customer or end users and which is compatible with the efficient operation of the Network, does not interfere with the services of other parties, does not result in inefficient or excessive use of the Network or the networks of Company's roaming carriers, and is not inconsistent with Network policies and practices.

1.3 "Approved Device" means a Device that has been certified and approved by Company.

1.4 "Area(s)" means the areas within the United States where Company is licensed to provide the Service and is providing Service. The Area may change from time to time.

1.5 "Device" means the equipment used by a Customer to originate or receive wireless transmissions on the Network, including any machine to machine communications unit, wireless modem, SIM, and any accessories. Cellular telephone(s) are expressly excluded from this definition.

1.6 "Equipment" means all equipment (other than equipment comprising portions of the Network) necessary to enable Customer to use or benefit from the Service, including but not limited to Customer's network facilities and any Device.

1.7 "Events of Default" means the following: (i) the execution of any assignment for the benefit of creditors or the filing for relief by either Party under any applicable bankruptcy, reorganization, moratorium, or similar debtor relief; (ii) the appointment of a receiver for Customer or Company or for substantially all of their respective assets or properties; (iii) Customer's failure to pay any sum owed to the other hereunder at the time such amount comes due; (iv) either Party's failure to perform or observe any other term, condition, or covenant to be performed by it under this Agreement; (v) an unauthorized assignment of this Agreement; or (vi) Customer's failure to utilize Equipment compatible with the Network or other network of Company, as determined by Company.

1.8 "Hosting Services" means access to the iQ2® / iQCommSentry® interface (as applicable), together with certain additional related services which may include private cellular network access, periodic firmware upgrades to the Service Devices (when necessary), temporary storage of Customer data, hosting of Customer remote-site web pages(s) (when applicable), remote troubleshooting, user-access management, carrier support and twenty-four (24) hour customer service. In certain cases, Hosting Services may also include custom Virtual Private Network configuration and maintenance, content filtering, usage monitoring and limiting, data pooling, network architecture and configuration assistance, transmission of data log(s) to Customer, site-to-site communication and alarm messaging.

1.9 "Machine to Machine Communications" means wireless communications made possible by the provisioning of an Approved Device or the insertion of a SIM by Customer or its agent into an Approved Device (as applicable) for use with an Acceptable Application upon activation of the Service, for use by Customer.

1.10 "Network" means those integrated mobile switching facilities, servers, cell sites, connections, billing systems and other related facilities used by Company to provide Service in an Area.

1.11 "Service" means the Hosting Services, and any machine to machine data and SMS wireless telecommunications services (as and where available) for GSM communications, GPRS (General Packet Radio Services), EDGE, Universal Mobile Telephone Service (UMTS), High Speed Packet Access (HSPA) Service, High Speed Packet

Access + (HSPA+), Code Division Multiple Access Service (CDMA), Enhanced Voice-Data Optimized Service (EVDO) or Long Term Evolution (LTE) technology. Service does not include any voice service.

1.12 "Service Plan" means the particular set of rates, terms and conditions as stated in the Exhibits to this Agreement upon which Company makes Service available to Customer, but does not include any short-term marketing promotions that may periodically be offered by Company.

1.13 "Subscriber Identity Module ("SIM")" means a specially programmed microchip that is inserted into a Device which encrypts transmissions and identifies the user to the Network.

1.14 "Subscription Fraud" means using or assisting another to use any scheme, false representation, or false credit device, or other fraudulent means or devices in connection with Service or any Service Device.

1.15 "Unauthorized Access" means any unauthorized use of the Service or any Service Device, which includes the practices generally referred to as "counterfeiting," "cloning fraud," or "tumbling fraud."

TERMS AND CONDITIONS

Section 2. Purchase and Sale of the Service. Customer agrees to purchase from Company, and Company agrees to sell to Customer, the Service for use in Machine to Machine Communications on Company's wireless Network as stated in the Exhibits hereto. The Service is provided to Customer for Customer's use and not for resale. The Service (other than roaming service) is only available in the Area. At all times Customer will comply with Company policies and procedures reasonably established by Company for providing the Service, and Company may from time to time modify these policies and procedures.

Section 3. Term. This Agreement commences on the Effective Date and remains in effect for the length of the Agreement Period as both are identified in Exhibit A attached hereto and incorporated herein by reference (the "Term"). This Agreement will automatically renew for successive one (1) year renewal Term(s) unless either Party provides the other with a notice of termination at least thirty (30) days prior to the end of the then-current Term.

Section 4. The Service.

4.1 Network Connections. Customer must connect to the Network in order to receive the Service. Such connections may be obtained under this Agreement or pursuant to separate agreement between the Parties.

4.2 General Service Requirements. Company will only activate Service for use with the Acceptable Applications and Approved Device(s). Company may require a minimum number of Device(s) to be activated at one time. To the extent that SIMs are required for Service, Customer is only authorized to purchase SIMs directly from Company or through Company's Affiliate(s) for use on the Network. Unless otherwise stated, an Approved Device, an Acceptable Application(s) and a SIM (when applicable) are required for all Service Plans. Company may, at its option, require Customer to provide information about how their applications interact with the Network, and may limit, restrict or prohibit use of applications in Company's sole discretion.

4.3 Service Requiring Use of SIMs. A number may not be associated with more than one SIM at the same time, unless otherwise approved by Company. Company may deny Service to any SIM(s) without liability to Customer for SIMs appearing on Company's service deny lists for reasons including, but not limited to, cases where the SIM is stolen, has been used for fraudulent purposes, is not used in an Approved Device or with an Acceptable Application, or is defective, and Company will notify Customer in such cases. Customer must not insert any SIM into anything other than an Approved Device, and/or program, re-program or tamper with any SIM in any manner, and Customer shall be responsible for the payment of any and all charges incurred resulting from any violation of this Agreement.

4.4 Modification or Termination of Service. If Customer desires to modify or terminate any Service or change Service Plans, Customer must advise Company in writing accordingly. Changes will become effective as determined by Company. Should Customer terminate Service under this Agreement at any time during the Term (or any renewal thereof as provided in Section 3), Customer shall pay to Company an early termination fee in an amount equal to fifty percent (50%) of the total balance of the Service Plan for the remaining current Term.

4.5 Troubleshooting. Customer will cooperate with Company in any troubleshooting of the Equipment or the Network as required to maintain the efficient operation of the Service.

4.6 Limitations on Roaming Service.

4.6.1 THE AVAILABILITY OF ROAMING SERVICES, AND THE CHARGES FOR THOSE SERVICES, IS DEPENDENT IN PART ON THE TYPE OF EQUIPMENT USED BY CUSTOMER AND THE PROGRAMMING OF THAT EQUIPMENT. COMPANY MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE AVAILABILITY OR QUALITY OF ROAMING SERVICE PROVIDED BY OTHER WIRELESS NETWORKS, AND COMPANY WILL NOT BE LIABLE IN ANY CAPACITY FOR ANY ERRORS, OUTAGES, OR FAILURES OF ROAMING SERVICES PROVIDED BY OTHER WIRELESS NETWORKS.

4.6.2 IF COMPANY, OR ANOTHER ENTITY WITH WHOM COMPANY HAS A ROAMING AGREEMENT, DISCOVERS OR SUSPECTS ABUSE OR FRAUD WITH RESPECT TO CERTAIN NUMBERS, THEN ROAMING PRIVILEGES MAY BE SUSPENDED WITH RESPECT TO SUCH NUMBERS. COMPANY WILL USE COMMERCIALY REASONABLE EFFORTS TO PROVIDE CUSTOMER WITH PRIOR, OR PROMPT SUBSEQUENT, NOTIFICATION OF THE SUSPENSION OF THE ROAMING SERVICE. COMPANY WILL NOT BE LIABLE IN ANY CAPACITY TO CUSTOMER FOR THE UNAVAILABILITY OR SUSPENSION OF ROAMING SERVICE BY OTHER CARRIERS.

4.6.3 TO THE EXTENT ACCESS TO ROAMING CAPABILITIES IS PROVIDED BY COMPANY TO CUSTOMER, IT IS DEEMED TO BE A "SERVICE" AS DEFINED IN SECTION 1, AND THE USE OF SUCH ROAMING BY CUSTOMER WILL BE GOVERNED BY THE PROVISIONS OF THIS AGREEMENT.

4.7 Service Technology Disclosures. The underlying carrier is not obligated to maintain any particular technology, and Network technologies may be terminated at any time in its sole discretion. Company will provide Customer twelve (12) months prior written notice of any termination of a significant wireless technology on a nationwide basis.

4.8 International Roaming. Service is not permitted to be used under this Agreement for international roaming, except on a rare and incidental basis. Should Company, in its sole discretion, determine that Customer is utilizing international roaming more frequently than on a rare and incidental basis, Company may terminate such international roaming with or without notice to Customer of such termination. With respect to any international roaming under this Agreement, Customer (i) shall provide Company with all assistance reasonably required to enable Company to comply with requests or requirements of a roaming carrier, regulator, or other governmental body relating to Customer's use of international roaming; (ii) shall comply with each country's legal and regulatory requirements arising from or relating to Customer's use of the Service; (iii) shall provide Company with the place of primary use of the Service (which must be its business street address and be within an eligible Company wireless Service area); (iv) expressly acknowledges that Service may not be available outside of a provisioned roaming zone; and (v) shall indemnify and hold Company harmless from any claims, costs, losses or damages resulting from Customer's international roaming.

4.9 PRIVACY. THE NETWORK HAS MANY COMPLEX ELEMENTS AND IS NOT GUARANTEED AGAINST EAVESDROPPERS, HACKERS, DENIAL OF SERVICE ATTACKS, VIRUSES, OR INTERCEPTORS. CUSTOMER AGREES THAT COMPANY WILL NOT BE LIABLE TO CUSTOMER OR TO END USERS FOR ANY LACK OF PRIVACY OR SECURITY. IN THE EVENT THAT CUSTOMER SUBSCRIBES TO AN UNMANAGED SERVICES PLAN, CUSTOMER EXPRESLY ACKNOWLEDGES AND AGREES THAT CUSTOMER SHALL BE SOLELY REPONSIBLE FOR ANY AND ALL SECURITY AND DATA MONITORING ASSOCIATED WITH SUCH SERVICE PLAN.

Section 5. DISCLOSURE AND ACKNOWLEDGMENT. CUSTOMER UNDERSTANDS AND AGREES (I) THAT CUSTOMER HAS NO CONTRACTUAL RELATIONSHIP WITH THE UNDERLYING WIRELESS SERVICE CARRIER/PROVIDER; (II) THAT CUSTOMER IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN COMPANY AND THE UNDERLYING CARRIER/PROVIDER; (III) THAT THE UNDERLYING CARRIER/PROVIDER HAS NO LEGAL OR EQUITABLE LIABILITY OF ANY KIND TO CUSTOMER WHATSOEVER, WHETHER FOR BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE, AND CUSTOMER HEREBY WAIVES ANY AND ALL CLAIMS OR DEMANDS THEREFORE; (IV) THAT MESSAGES MAY BE DELAYED, DELETED OR NOT DELIVERED; AND (V) THAT THE UNDERLYING CARRIER CANNOT GUARANTEE THE SECURITY OF WIRELESS TRANSMISSIONS AND WILL NOT BE LIABLE FOR ANY LACK OF SECURITY RELATING TO THE USE OF THE SERVICES.

Section 6. Rates.

6.1 Service Plans. Customer will pay for Service at the rates set forth in the applicable Service Plan(s) as selected by Customer. Rate plan changes will take effect as stated in the Exhibits. Company may modify a Service Plan or charge at any time by providing thirty (30) days advance written notice to Customer, provided that any modification not adverse to Customer may be made immediately effective upon written notice.

6.2 Service Outages. In the event of a total Service outage within an Area which is not caused by Customer and which lasts for a period of twenty-four (24) hours or more, a credit allowance will be made at Customer's request in the form of a pro rata adjustment of the fixed charges billed by Company to Customer with respect to the affected SIM(s). Periods of discontinuous outage may not be accumulated in determining if an outage has continued for at least twenty-four (24) hours. In order to receive such credit, Customer must submit a written request to Company, stating the date and location of the outage, the SIMs affected, and such other information as Company may reasonably require. Such notice must be received by Company within ten (10) business days following the last date of the period of outage. EXCEPT AS PROVIDED HEREIN, COMPANY WILL NOT INCUR ANY LIABILITY OF ANY NATURE OR TYPE WHATSOEVER FOR SERVICE OUTAGES.

Section 7. Invoices, Payments, Disputed Charges and Billing Data.

7.1 Invoices and Billing Data. Company will provide Customer a summary invoice for all charges on a monthly basis, normally within ten (10) days subsequent to the cut-off date for each billing cycle, each such invoice containing all charges and applicable taxes and/or regulatory fees. All SIMs will be placed on the same billing cycle. Customer must notify Company if Customer has not received an invoice within twenty (20) days subsequent to the bill cycle cut-off date. Company will use reasonable efforts to provide electronic detailed billing data for all Service Plans loaded into a billing cycle.

7.2 Payments. Payment in full for each invoice is due at the location set forth in the invoice, in a form payable in U.S. currency, upon the due date set forth in the invoice or within thirty (30) days subsequent to receipt of the billing data (which shall include any amounts due for data usage in excess of the allotted amount for the then-current billing period), whichever is later (the "Due Date"). For purposes of payment, Customer may rely only on the invoice and other billing data received from Company, and may not rely on any other source including information drawn from any Company or Customer system. Depending on Customer's payment history, Company may at its sole discretion require payment by certified check, money order, or wire transfer. Payments are past due, and Customer will have committed an Event of Default, if not received by the Due Date. Time is of the essence with respect to payment of Company's invoices. If a payment becomes past due, the account will accrue late fees and interest at the rate of one and one-half percent (1.50%) per month or the maximum lawful rate, whichever is greater. Customer agrees not to place any condition or restrictive legend, such as "Paid in Full", on any check or financial instrument used to make a payment. The Parties agree that the negotiation of any such check or instrument so inscribed will not constitute an accord and satisfaction or novation.

7.2.1 Suspension of Service. In the event that Customer fails to timely make payments to Company as required in this Agreement, Company may suspend the Service at any time. During the pendency of any suspension of Service, all charges, fees and taxes for Service will continue to accrue, and Customer will continue to be financially responsible for the payment of such amounts. In order to restore any suspended Service, Customer shall pay a reactivation fee in the additional amount of One Hundred United States Dollars (\$100.00) per Device.

7.3 Disputed Charges. If Customer disputes part of the monthly invoice, Customer is required to notify Company in writing and to submit appropriate documentation justifying such dispute to Company as soon as it is aware of the dispute, but in no event later than the thirty (30) days after the invoice Due Date or such dispute is waived. Notwithstanding any such dispute, Customer agrees to pay the full amount of any such bill pending the resolution of such dispute. Company will respond to Customer's written dispute within thirty (30) days of receipt of such dispute. Company and Customer agree to use best efforts to resolve all disputes and Company agrees to promptly refund any amounts due upon dispute resolution. The notice requirements in this Paragraph 7.3 will not shorten the period within which actions must be filed as established by the applicable statute of limitations, but will constitute a condition precedent to any right of the aggrieved Party to contest prior invoices or payments. This condition is designed to allow each Party the opportunity to preserve important evidence in defense of a claim.

Section 8. Abusive or Fraudulent Use.

8.1 Generally. Service may be restricted or cancelled if there is a reasonable suspicion of abuse or fraudulent use. Company will provide prompt notice of the restriction or termination to Customer. Customer agrees to make good faith efforts to minimize abuse or fraudulent use, to promptly report to Company any such abuse or fraudulent

use of which Customer becomes aware, and to cooperate in any investigation or prosecution initiated by Company. Customer also agrees that Company may in its discretion disable any Device, or otherwise block access to the Service when suspected of abuse or fraudulent use. Abuse and fraudulent use of Service include, but are not limited to (i) attempting or assisting another to access, alter, or interfere with the communications of and/or information about another wireless customer; (ii) tampering with or making an unauthorized connection to the Network; (iii) installing any amplifiers, enhancers, repeaters, or other devices that modify the radio frequencies used to provide the Service; (iv) Subscription Fraud; (v) using Service in such a manner so as to interfere unreasonably with the use of Service by one or more other wireless customers or to interfere unreasonably with Company's ability to provide Service; (vi) using Service to convey obscene, salacious, or unlawful information; (vii) using Service without permission on a stolen or lost Device; (viii) Unauthorized Access; (ix) using the Service to provide voice over IP services; and/or (x) extensive use of the Service outside of the Area.

8.2 Liability for Abuse or Fraudulent Usage. Customer is solely liable for charges, costs and damages resulting from (i) Subscription Fraud, (ii) any theft of a Device, any user identification number, or password associated with the Service; (iii) any abuse or fraud facilitated by Customer, Customer's employees, or Customer's agents, and/or (iv) any failure to give prompt notice of suspected abuse or fraudulent use based on information available to Customer.

Section 9. Limitation of Liability.

9.1 Generally. COMPANY'S ENTIRE LIABILITY, AND CUSTOMER'S EXCLUSIVE REMEDY, FOR DAMAGES ARISING OUT OF MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, LOSS OR CORRUPTION OF CUSTOMER'S DATA, ERRORS OR DEFECTS IN THE SERVICE(S), SHALL IN NO EVENT EXCEED THE SPECIFIED CREDITS UNDER THIS AGREEMENT, OR IF NO CREDITS ARE SPECIFIED, AN AMOUNT EQUIVALENT TO THE PROPORTIONATE CHARGE TO CUSTOMER FOR THE PERIOD OF SERVICE DURING WHICH SUCH MISTAKE, OMISSION, INTERRUPTION, DELAY, ERROR OR DEFECT IN THE SERVICES OCCURS AND CONTINUES. IN NO EVENT SHALL ANY OTHER LIABILITY ATTACH TO COMPANY.

9.2 Consequential Damages. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES, OR INCREASED COST OF OPERATIONS.

Section 10. Default and Termination.

10.1 Default. This Agreement may be terminated upon an Event of Default by either Party if such Event of Default is not cured by the defaulting Party within thirty (30) days subsequent to receipt of a notice of the Default; provided, however, that in the case of failure to pay invoices or in the case of a violation of Section 8 of this Agreement, this Agreement may be terminated if such Event of Default is not cured within ten (10) days subsequent to receipt of notice of the Event of Default.

10.2 Termination for Convenience. Company may terminate this Agreement at its convenience upon ninety (90) days' prior written notice to Customer.

Section 11. Installation Services Warranty. The Installation Services Warranty applies to all work performed by Company in connection with the establishment of the Service (the "Installation Services"). Company warrants and represents that the Installation Services shall be free from any material defect for a period of one (1) year subsequent to the commencement of the initial Term of this Agreement (the "Installation Services Warranty Period"). In the event that Customer notifies Company during the Installation Services Warranty Period that a defect in the Installation Services exists, Company agrees to provide such services as are reasonably necessary to correct said defect in the Installation Services at no cost to Customer; provided, however, that in the event Company in good faith determines that the alleged defect is not due to any fault of Company, or if Customer's notice is tendered subsequent to the expiration of the Installation Services Warranty Period, then Customer shall pay Company for all services provided to Customer in accordance with Company's then-current rate schedule. The Installation Services Warranty only applies to defects in the Installation Services and not defects in any Device(s) or Equipment, or defects caused by other circumstances, including without limitation accident, misuse, unforeseeable use, neglect, alteration, vandalism, improper installation by others, improper testing, improper repair and/or Acts of God.

Section 12. Other Provisions. All notices and other communications under this Agreement shall be in writing and shall be deemed given when delivered personally, transmitted by facsimile (provided that a copy of such facsimile is sent by certified mail, return receipt requested) or sent by certified mail, return receipt requested, to the Parties

address(es) of record. Time is of the essence of each of the provisions of this Agreement. Customer shall not assign, transfer or encumber this Agreement without obtaining prior written consent of Company, nor shall any attempted assignment, transfer or encumbrance of this Agreement be effectuated by operation of law or otherwise without the prior written consent of Company. Company may assign or transfer this Agreement to any Affiliate without obtaining consent from Customer, written or otherwise, and such assignment or transfer shall be effective immediately upon execution and delivery by Company. The person executing this Agreement on behalf of Customer expressly warrants and represents that he/she is the authorized representative of Customer and possesses the requisite authority to legally bind Customer to the terms and conditions hereof. The Parties hereto expressly acknowledge and agree that (i) except as otherwise expressly set forth herein, no representation(s) has been made with respect to the subject matter of this Agreement, nor any representations inducing the execution and delivery of this Agreement, (ii) each Party has relied on such Party's own judgment in entering into this Agreement, and (iii) any statements and/or representations that may have been made previously by either of them to the other are void and of no effect, and that neither of them has relied upon such statements and/or representations in connection with such Party's dealings with the other. The Parties expressly agree that it is their intention and covenant that (A) this Agreement, any performance under this Agreement, and all suits and proceedings arising out of, related to, in connection with or by reason of this Agreement, be construed in accordance with, and under and pursuant to, the laws of the State of Mississippi; (B) the laws of the State of Mississippi will be applicable and will govern any action or other proceeding that may be brought arising out of, related to, in connection with or by reason of this Agreement, to the exclusion of the law of any other forum; (C) unless expressly waived by Company, the exclusive jurisdiction and venue of any legal action with respect to the subject matter of this Agreement shall be the appropriate Court for Rankin County, Mississippi, and (D) each of the Parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such legal action. If it becomes necessary for any Party to undertake any litigation or to employ an attorney to assist such Party in pursuit of or protection of its rights under this Agreement, the non-prevailing Party shall be obligated to reimburse the prevailing Party for such fees and related costs and expenses, including reasonable attorney's fees, whether incurred at trial, on appeal, or otherwise. The invalidity, illegality, or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if such invalid, illegal, or unenforceable provision had been omitted. This Agreement shall not be amended or modified, and none of the provisions hereof shall be waived, except in a writing signed on behalf of the Parties hereto or, in the case of a waiver, on behalf of the Party making the waiver. All terms and conditions of this Agreement shall be binding upon the successors and assigns of the Parties hereto. No waiver of any provision of this Agreement shall be implied by any failure of either Party to enforce any remedy upon the violation of such provision, even if such violation is continued or repeated subsequently. No express waiver shall affect any provision other than the one specified in such waiver, and that only for the time and in the manner specifically stated. This Agreement may be executed in any number of copies, each of which shall be deemed an original and no other copy need be produced. Captions to and headings of the Sections and Paragraphs of this Agreement are solely for the convenience of the Parties and shall not be used for the interpretation or determination of the validity of the Agreement and/or any provision(s) hereof. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine, neuter, singular or plural as the identity of the person or persons may require.

COMPANY:

CUSTOMER:

LEC, INC.

A Mississippi Business Corporation

Name of Company



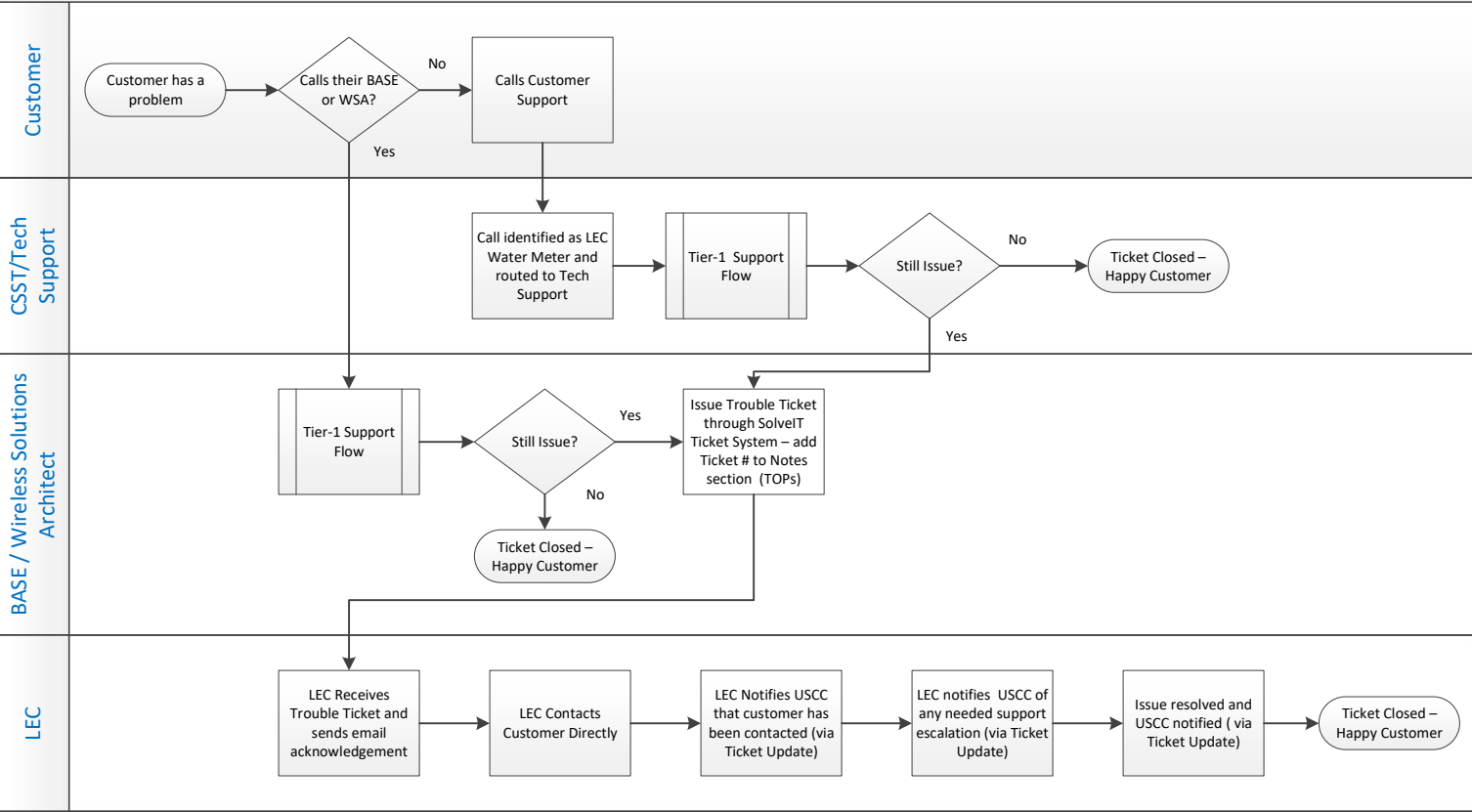
By: _____
Authorized Representative
(Signature)

Authorized Representative
(Signature)

Title

Smart Water Meter Cellular Endpoint - Troubleshooting

Phase



Leaders In Industrial Automation Control Engineering and IIoT Communication



Leaders in Industrial Automation
Control Engineering and
IIoT Communication



Our Applications

In the ever-evolving motion-control and electric motor industry, LEC's international experience in developing components, engineering systems and programming software for clients spans a vast array of verticals. Our broad client portfolio ranges from oil & gas, pipeline and transportation companies to water/wastewater, forestry and many more key industries.



Oil & Gas, Pipeline

- Drilling Rig Remote Monitoring Systems
- Production Monitoring Systems
- Pumping Unit Monitoring Systems
- Pipeline Metering Station Monitoring and Control Systems
- Pipeline Control and Block Valve Controls and Monitoring Systems
- Pipeline SCADA Systems



Water / Wastewater

- Wastewater Pump Stations
- Potable Water Well Controls
- Elevated Tank Controls
- Treatment Process Controls



Metals & Machining

- C-N-C Machining
- Arc Furnaces
- Punch Presses
- Rolling/Stamping/Slitting
- Die Casting
- Draw Blocks
- Annealing



Forestry / Agriculture

- Bucking, Sawing & Chipping
- Trimming, Sorting & Stacking
- Drying & Packaging



Power Generation

- Fuel Tank Farm Supervisory Control
- Process Water Filtration & Treatment
- Wastewater Filtration & Treatment
- Electrostatic Precipitator Controls
- Bottom Ash Control Systems
- Fly Ash Control Systems
- Hydro-Electric Generator Controls
- Raw Water Intake Controls



Robotics

- Pick & Place
- Welding
- Assembly



Communications

- Ethernet Networks
- VPN Access
- ControlNET
- DeviceNET
- Modbus / RS485
- Fiber Optic
- Cellular
- Internet



Monitoring

- SCADA Systems
- Remote Monitoring Systems
- Residual Chlorine Monitoring Systems



Automotive

- Tire Industry
- Welding Machines
- Component Assembly
- Automation
- Quality Control - Vision
- Inspection Systems



Plastics

- Injection Molding
- Extruding
- Blow Molding
- Thermoforming
- Ultra-Sonic Welding



Food & Beverage

- Batching
- Ovens
- Fillers/Seamers/Cappers
- Packaging
- Palletizers
- Bar Coding/Sorting



Chemical

- Custom Container Filling Stations
- Palletizers
- Batch Controllers



Paper Industry

- Paper & Pulp
- Converting
- Presses



Fiber Glass Insulation Production

- SMC Production
- 10 & 15 Ton Presses



Transportation

- Draw Bridge Controls
- Bridge Automation



Amusement & Entertainment

- Roller Coaster Automation
- Water Park Automation

LEC Is Engineering Smarter Systems

LEC supplies the competitive advantage to industry, turning challenging circumstances into revenue-generating results by providing the cutting-edge production and process management automation tools needed to face competitors head-on in a demanding global marketplace. Our proven experience is demonstrated via our clients' success in areas such as cost reduction, higher-quality manufacturing, process efficiency increase, greater employee safety and productivity improvement.



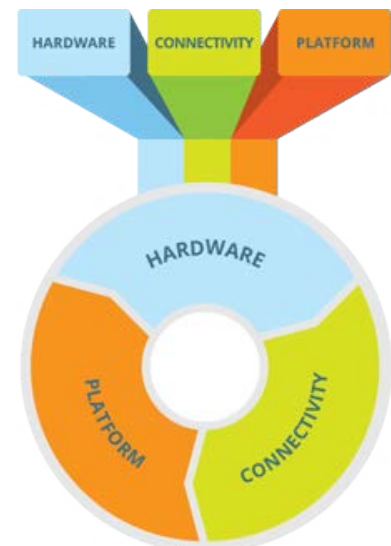
Who We Are

LEC provides industrial automation and control engineering, and industrial IIoT enablement and cloud platform services of the highest quality. Every day, we demonstrate an unending commitment to our clients, strategic partners and communities.

Automation is a crucial element of the manufacturing and production process. The efficiency of any process is dependent on successful system integration. LEC supplies the competitive advantage to industry, turning challenging circumstances into revenue-generating results. We provide the cutting-edge production and process management automation tools needed to face competitors head-on. LEC produces tangible benefits - cost reduction, higher-quality manufacturing, process efficiency increases, greater employee safety and productivity improvement.

Access to our professionals is not restricted to "traditional" business hours and workdays. Our highly experienced emergency support teams are available any time – day or night. By incorporating remote access features into your control system, our teams are enabled to diagnose issues, and in many cases remedy them from virtually anywhere.

Additionally, we offer our clients the option of attending customized training sessions, either on-site or in a hands-on classroom environment.



Proven Industry Leaders

Our passion is engineering smarter systems that exceed expectations. LEC's experienced and passionate team brings a multidisciplinary approach to addressing the challenges that affect our clients. We're setting a new standard in industrial automation control engineering and IIoT enablement.



Strategic Partner Alliances

LEC's well-established strategic alliances with industry leading component manufacturers, hardware providers, network carriers and platform developers enable our team to successfully design, produce, and integrate custom systems based on the specific, individual needs of each client. These Alliances play a vital role in LEC's consistent delivery of successful results.

Experienced Human Resources Behind the Technology

The core of our flexible workforce includes engineers experienced in a variety of disciplines with the knowledge to complete a project of any size and in nearly any industrial application. Our professionals are passionate about design, fluent with technology, and engaged in each aspect of every project.

- Automation Engineers
- Industrial Engineers
- Network Architects
- Electrical Engineers
- Mechanical Engineers
- Computer Engineers
- Civil Engineers
- Network Engineers
- PLC/Automation Programmers
- Certified Panel Technicians



Engineering Products & Services

Engineering & Consultation

Consulting services offered by LEC range from specification of a single system component to turnkey design-build services. We have an extensive network of resources, both technical and non-technical, which allows us to accommodate client needs during any phase of a project. These services are not specific to any particular market segment and are applicable to both public and private-sector projects. LEC provides the solutions needed as well as the documentation required to keep up with all details of a project; including schematics, hardware/software manuals, and fabrication details. All of our documents are accurate, easy to follow, and simple to modify.



Industrial Automation & Control Systems

LEC's team has decades of experience in engineering smarter automation systems for industry, delivering real solutions to successfully solve critical process and control application challenges. We are committed to the continuous training of our team and to the innovation advancement of our industrial automation services. Whether you need a single-station work cell, a completely integrated multi-functional assembly line, or the integration of new components into an existing system, LEC has the solution. Our team of experienced engineers, programmers, technicians, and software developers focuses on providing cost-effective solutions. Clients rely on us for process integration, machine design and build, PLC and RTU programming, HMI SCADA development, production monitoring and reporting, data collection, servo and VFD programming, machine diagnostics and alarming, panel design, and industrial IoT solutions.

Systems Integration

LEC's experienced team of control system integrators design and implement sophisticated control systems for manufacturing operations, process and other industrial facilities. We leverage our extensive knowledge of engineering, information technology, operations, and business to expertly integrate plant equipment to automate manufacturing and processes from the plant floor to the enterprise level. Automation helps manufacturers and processors reduce cost, increase production, use less energy and lower environmental impact. Our extensive experience with a vast array of hardware and software platforms and their unique communication protocols enables us to effectively integrate multiple machine control systems in accordance with specific client requirements, whether into a comprehensive control room, SCADA application, or cloud-based solution.





Engineering Products & Services

UL-508A Certified Industrial Panel Design & Fabrication

LEC specializes in providing custom control panel solutions of the highest caliber in the manufacturing industry with a proven track record of satisfying a variety of industrial automation needs. Our team of highly experienced technicians expertly construct control panels to the highest quality of industry standards using the best products from trusted hardware manufacturers. LEC's UL-508A Certified Panel Shop can accommodate any size project, and provide engineering support from design concept to completion.



Skid Design & Fabrication

Our engineers, technicians and fabrication teams provide the best quality skid-mounted measurement technologies and mechanical and electrical controls available in the industry. LEC's professionals can manage and advise on your project from initial design through start-up and commissioning. We offer both standard designs for quick turnaround to meet tight deadlines, and customizable solutions to meet unique regional or application requirements.





Programming

PLC Programming

Our skilled professionals provide software programming services for a variety of brands of Programmable Logic Controllers (PLCs). Our software development outcomes are easy to use, organized, and simplified, with descriptive comments to give our clients the information they need to maintain their equipment.

HMI & Operator Interface Programming

Regardless of the complexity of your HMI needs, LEC provides sophisticated, user-friendly systems that are easy to operate, and our professionals are experienced in designing and programming a wide variety of operator interface systems.

Motion Control Programming

We are skilled in the design, installation, and commissioning of an extensive array of motion-control components and variable speed drives, which provide smooth operation of electronic gearing, contouring, and circular motion applications.



Radio Frequency Controls

LEC has extensive experience in providing solutions utilizing a variety of wireless controls and I/O devices in accordance with your particular requirements. These are crucial when an application involves potentially dangerous machinery (such as conveyors and blenders) or the monitoring of equipment, motors and other devices from a remote location.



Programming

Industrial Internet of Things Enablement Products and Services

LEC offers experienced Industrial Internet of Things (IIoT) enablement, filling the gaps between disparate technologies.

- Integrating existing field devices and assets into a current IIoT framework.
- Connecting disparate systems into a single platform and user interface for monitoring and control.
- Developing ground-up, custom IIoT solutions to meet specific client requirements.
- Long-term solution support to ensure sustainability while meeting ongoing and future IIoT business needs.



Mission Critical IIoT Connectivity

- Highly secure and redundant wireless connectivity
- Advanced private network with client access to real-time network analytics
- Managed services staffed with skilled support and troubleshoot personnel
- Pre-commissioned hardware for optimized deployments
- 4G LTE Network
- System Consulting & Design
- Robust 24/7 ticketing system with solveIT™ support tool



Engineering the Components of IIoT

LEC offers experienced Industrial Internet of Things (IIoT) enablement, filling the gaps between disparate technologies. With years of industrial controls and automation experience, along with investment in new and innovative technologies and the brightest human resources, LEC is truly a market leader in deploying IIoT. Trusted by the industry, wireless carriers and enterprise clients alike, LEC is a proven partner in business.

Visualization & Control Through Robust IIoT Platform Technologies

- IIoT platforms delivering data visualization, analytics, and control
- Reliable alarm and fault notification systems
- Ability to extract data and enable control both remotely and in-plant
- Data logging and reporting functionality
- Simple configuration and intuitive user interface
- Access from any browser-enabled device



Introducing iQ2™. Intelligence. Squared.

iQ2 is LEC's complete, end-to-end IIoT platform solution, designed from an industrial automation engineering perspective, to effectively and efficiently address individual needs. Our flexible IIoT integration process quickly and easily enables our cutting-edge platform technology on the plant floor, for OEMs and any industrial remote assets.



ENABLING IIoT

Engineering the Components of IIoT



iQ Web SCADA

LEC's complete end-to-end monitoring and control solution, iQ Web SCADA, integrates into almost any new or existing control or automation system regardless of the function of the machinery, equipment, or system. The iQ Web SCADA platform can be used all or in part, depending on the needs of the user.



iQ CommSentry

LEC's iQ CommSentry service tool provides users with a simple solution to monitor and manage network performance resulting in reduced downtime and the prevention of costly errors. This platform simplifies compliance management, IP address management, easily tracks and locates network users and devices, and analyzes network traffic and bandwidth usage.



COMMSENTRY
MANAGING IIoT

Support



Technical Support Center

LEC's newly-launched, cutting-edge solveIT™ Technical Support Center provides clients with direct, 24/7 access to data, project information and support request updates using the latest technology compatible with today's browsers and mobile devices. solveIT™ is a user-friendly and highly-collaborative cloud-based system designed to give clients instant access to detailed information regardless of locale. solveIT™ features data sharing, client data input capabilities, support ticket tracking, project tracking, hardware information and much more, increasing overall project management effectiveness.

On-Site Support

Technical support is a crucial component of LEC's services, and we are always pleased to assist clients with on-site questions or maintenance needs.



Replacement Components

We have a commitment to providing every nature of support for our clients' systems throughout their service life. In addition to our remote assistance and on-site support services, we also offer replacement components for every aspect of control and automation systems.



**Leaders in Industrial Automation
Control Engineering and
IIoT Communication**

Appendix T

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory J: IoT Management

ConnectHQ powered by Nokia WING



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
ConnectHQ powered by Nokia WING
- b. General Application Area
Subcategory J: IoT Management
- c. General capabilities provided
ConnectHQ powered by Nokia WING is equipped to handle the present and ever-growing IoT reality. That means everything from utility meters, signboards, remote sensors, cameras and appliances are interconnected and need a centralized system to coordinate their activations, suspensions, data use, and billing reports. ConnectHQ is a Connected Device Platform built for larger scale operations as well as for those that do not have an in-house IT department. ConnectHQ can take away barriers to those wanting to maximize IoT solutions for their organization.

ConnectHQ is a self-service platform enabling business customers to manage connectivity for data-only devices. It provides a table stakes customer experience which offers:
 - Single and Bulk activation of devices
 - Data usage monitoring
 - Usage alerts and more
- d. Expected impact on cost/performance/functionality, etc.
With Connect HQ, users can optimize price plans to minimize costs. By managing devices through the Connect HQ on-line portal, you can manage data usage, suspend high usage devices and seasonally suspend devices that are not in use. Real-time reporting allows you to perform high-volume usage analysis to manage costs.
- e. Subcontractors/partners involved in delivering service
ConnectHQ is UScellular's IoT device management platform that is powered by Nokia WING.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
No, there are no End User Licensing Agreements associate with ConnectHQ.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
ConnectHQ's online portal drives the following benefits for organizations:
 - Remote activation and de-activation of devices.
 - Provides a self-service portal, lessening the chance that miscommunications occur that could delay day-today operations.
 - Remote device management, saving on previously time-consuming on-site visits.

- The setting of the type of information content and specifications produces information that is relevant to you.
 - Enables you to stay abreast of billing and data usage and visibility to past invoices, data usage, and account history.
 - Helps your company to keep on top of, and implement, price plans right for your business.
 - Crucially, when it comes to remote monitoring, CDPs have the capacity to alert you concerning device usage and status.
- b. Applicability to government needs
Manage IoT devices including routers, sensors, asset trackers, failover, etc. in one centralized system.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
We have approximately 185,000 subscribers in ConnectHQ today. A number of our Public Safety, Utility, Education and Government customers utilize ConnectHQ to manage IoT devices, including statewide customers.
- Reference:
State of Wisconsin (please see Attachment Q)
- d. Overall interoperability of turnkey system for government use
Access can be web-based or via API to integrate directly into internal (government) systems.
- e. Accessories available for turnkey offering
The on-line portal does not require any additional accessories.
- f. Thoroughness of the vetting process used to select partners
UScellular reviewed multiple vendors and vetted several options to select Nokia WING. Nokia WING met UScellular's expectations for functionality and ease of use from a customer, sales, engineering, IT and overall business perspective.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
UScellular built ConnectHQ in conjunction with Nokia WING. Thorough high level, low level design, vetted with all key departments within our organization. Performed progression/regression testing. UAT testing, friendly user trial to ensure the system meets our needs and the needs of our customers.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
Not required. Connect HQ is a web-based self-service portal that users log into for IoT data management.
- b. Project coordination
Our teams will work with customers on launching ConnectHQ through a thorough on-boarding process that includes training and assistance with initial set-up. The portal is self-service, and your UScellular support team is available for questions or assistance.
- c. Installation and Testing process
Not required. Connect HQ is a web-based self-service portal that users log into for IoT data management.
- d. Client Infrastructure and support assessment process
Not required. Connect HQ is a web-based self-service portal that users log into for IoT data management.
- e. End user Acceptance process
Not required. Connect HQ is a web-based self-service portal that users log into for IoT data management.
- f. Approach to maintenance and support
UScellular works directly with NokiaWING on maintenance. UScellular will provide communications and training for any updates that directly impact our customers.
- g. Initial and Ongoing Training provided
UScellular offers online training for ConnectHQ and a comprehensive user manual. Your UScellular support team is available for questions and on-going training.
- h. On-going support and enhancement over the life of the agreement
UScellular works with customers to launch ConnectHQ within their organization through a thorough on-boarding process that includes training and assistance with initial set-up. The portal is self-service, and your UScellular support team is available for questions or assistance.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
No additional services.
- b. Experience and qualifications of partners and subcontractors
Nokia WING facilitates operators to scale up 5G IoT services faster without additional infrastructure investments. With a global network presence, it helps operators monetize IoT opportunities across diversified industries such as connected cars, critical public services, healthcare and real-time industrial monitoring and control through unified orchestration and consistent service levels.
- c. Description of Additional Integration and Consulting Services provided
Depending on the chosen solution, additional consulting and integration services are available.

Attachment Q:
State of Wisconsin Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh
Subcategory J: IoT Management

Client Company name:	State of Wisconsin Department of Administration
Client name of contact:	Connie Bandt
Client contact title:	Section Chief-IT Investment Manager
Client is a daily user, occasional user, etc.:	Daily user

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Brynna Johnson no later than Thursday, October 29th. Please note that USCC will not receive points for unreturned questionnaires.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?
[For wireless phone service. At least since the mid-2000s.](#)
2. Would you recommend USCC to other customers? Why?
[Yes, I would recommend USCC to other customers. We are able to get service to places we needed it in within the state. Our account team meets with us and assists whenever we ask. They research and provide solution when we have a special request.](#)

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?
USCC has been able to coordinate and manage an installation that we need. They are very responsive to our requests and provide updates as they have them. Deadlines/milestones are met and if they can't be, they will explain why and how they are trying to meet them.
4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?
They continue to meet our expectations. For SLAs I can't think of time when USCC has not met them and we have had to have discussions regarding them not meeting them. I think one of the times that we were disappointed in USCC was when they change their billing system. It caused a huge delay in us being able to pay our invoices and bill our customers back. USCC worked with us individually to get the problem resolved so that we could get back on track.
5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?
Products have worked the way they should. Can't think of any area where it has fallen short of expectation. Maybe in throttle of data. But here again, they will take things back and see if there are work arounds or other plans to meet the business need or request we are asking for.
6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?
Right now the biggest thing is the throttling of data when you exceed a bandwidth limit. Not sure this is still a problem. But in the past this is something that has been asked by our customers.
7. Is there anything else you think we should know about working with USCC or using USCC's products and services?
We have had a change in account managers and senior leaders at USCC. No matter who comes on board, it is consistent on how they treat us and work with us. You don't always see that. Sometimes it gets worse when people change on your account. I have not seen that with USCC.
8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?
We are talking with them about the ability to provide VPN type of solution. The discussion is going well and they are providing ideas and solutions for us.

Appendix X

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Category M: Enterprise Messaging

Team on the Run by StreamWIDE



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
[Team on the Run by StreamWIDE](#)
- b. General Application Area
[Subcategory M: Enterprise Messaging](#)
- c. General capabilities provided
[Team on the Run is a business communication tool for smartphones, tablets, and PCs. It includes a secured and feature rich messaging function that enables organizations to have an all-in-one business communication to protect company information assets and facilitate collaboration among individuals and distributed teams.](#)

Key Team on the Run Secure Messaging Features:

- [Integrated contact list controlled by administrator; all clients are synchronized with most updated contact information across the organization.](#)
- [Functional groups defined by admin](#)
- [Ad-hoc groups created by user](#)
- [Secured messaging. The application applies NIST FIPS-140 compliant ciphering suites \(AES, RSA, SHA-256/SHA-384, ECDHE\) to encrypt all communications with the service](#)
- [Securely share documents](#)
- [Securely share pictures and videos](#)
- [Record and securely share audio clip](#)
- [Broadcast messages](#)
- [Universal search on conversation and contacts](#)
- [Message read receipt](#)
- [Message acknowledgement](#)
- [Mobile client for Android and iOS](#)
- [Web client](#)
- [Fully synchronized mobile and Web clients](#)

[Additional communication capabilities that complement secured messaging](#)

- [Secured Push-To talk function](#)
- [Secured VOIP calling function](#)
- [Geo-location tracking](#)
- [My business process and forms. \(requires My Business package\)](#)
- [SDK](#)

- d. Expected impact on cost/performance/functionality, etc.
[Team on the Run impacts and enhances organizations' performance in the following areas:](#)
 - [Increase productivity](#)
[Real time: check-ins, forms, meetings, info](#)
[Multimedia: photo and video of problems](#)
[On the run: sales, maintenance, contractors](#)

Minimize communication costs (Inmarsat, offshore, roaming)
Coordination
Personal use at work
Sense of belonging to the company
 Not every employee has a desk
 Temporary workforce

Secured/private collaboration
Executive communication
Business continuity enabler for distributed teams

Enable an all in one business communication tool
- Process management (requires My Business package)
- VOIP calling
- Push-To Talk communication
- Inter-organization communications

- Avoiding security breaches and associated fees & fines
Increase compliance
Some categories of personnel deal with extremely sensitive information
Other less sensitive information could become a threat if massively hacked and compiled
Consumer IP messaging is an easy way to cross boundaries between personal, public and professional consciously or not
It can be completely out of control and not match corporate obligations (SOX etc.)
Most OTT applications repeatedly prove to be vulnerable, and are directly linked to specific foreign countries hub (Whatsapp/USA, Wechat etc.)

For example, in a utility/energy organization a broken or damaged pipe can cost thousands of dollars per minute. Incidents can occur far away from maintenance/spare parts warehouse. Fast communication between field engineers and warehouse shorten repair time and save money.

- e. Subcontractors/partners involved in delivering service
UScellular distributes Team on the Run SaaS. Team on the Run is a product developed by StreamWIDE, the StreamWIDE team is responsible for implementation (delivery) and support.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes. Please see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described

Team on the Run allows organizations to:

- Enhance field and back office team's productivity
- Facilitate employee onboarding providing a single application to manage business communications
- Reduce security incidents
- Provide instant expertise sharing between remote teams
- Improve P&L
- Save on communication costs (SMS blast, roaming)
- Accelerate incident qualification reported on the field
- Have more accurate incident qualification due to multimedia sharing capabilities
- Achieve faster response and repair time
- Increase organization's customer satisfaction

- b. Applicability to government needs

Since data confidentiality and security are a key aspect of the government entity's communication process, Team on the Run provides secure and fully controlled environment to the local, state and federal government staff in the office or in the field; allowing them to communicate via smartphones and tablets. See above items to see how Team on the Run capabilities translate into organization benefits.

- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use. Provide references

UScellular provides Team on the Run to 30 active customers with over 400 licenses.

StreamWIDE has 150+ organizations utilizing Team on the Run SaaS in US with a total of 10,000+ active end users.

Some specific Team on the Run relevant customers:

Municipalities

City of Oldbridge Township
Downtown Schenectady
Downtown DC
Tampa Downtown

School districts

Vallejo Unified school district
Washington Unified school district
Richmond Public school VA

- d. Overall interoperability of turnkey system for government use

With its key features, 99.999% guaranteed uptime SLA and military-grade secured communication Team on the Run is capable of fulfilling any state, local and federal government secure messaging needs.

The solution is deployed on a SaaS/ cloud model and requires:

- Mobile devices Android / iOS with 3G/4G/5G data plan for mobile users
- Desktop with Chrome/Firefox browser for Web administration or Web client

e. Accessories available for turnkey offering

Team on the Run comes as Software as a Service (SaaS) and works on mobile devices such as smartphones and tablets and PCs. In addition, Team on the Run works with several device and accessory providers such as Samsung, Sonim, Kyocera providing its services on ruggedized devices, tablets, etc.

Team on the Run also has integration with multiple accessories to enhance the push-to-talk service with RSM and emergency buttons.

- Pryme BT-PTT-Z MINI
- Aina wireless RSM – PTT
- Aina wireless button for emergency
- Klein Valor RSM
- Raxon BT-24HC
- Savox SH-01
- Stone Mountain Phoenix
- Savox
- Klein Drift PTT Earpiece
- Klein Triumph 1-Wire

Compatibility matrix of the above accessories with Android and iOS devices can be provided upon request

f. Thoroughness of the vetting process used to select partners

A thorough industry analysis and full RFP process were used to select StreamWIDE as UScellular's solution provider. StreamWIDE has been recognized among the players within the industry being an expert in carrier-grade telecom solutions serving 130+operators, 100M+ End-Users worldwide with live operations in 71 countries / 5 continents.

g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

The solution has been tested in both UScellular and StreamWIDE labs for integration with related UScellular solutions, such as UScellular provided mobile devices (Android and IOS smartphones, tablets, etc.). The solution is in use both internally and deployed with many UScellular customers.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

a. Pre-installation coordination

Team on the Run installation will be supported by StreamWIDE and UScellular teams. The following are important elements to work before the solution is deployed

- Understand the customer problem
- Define how Team on the Run will contribute to the solution of problem
- Identify use cases and user roles (admin, dispatcher, users)
- Identify the need of accessories
- Gather user phone numbers to configure and device types (Android / iPhone)

UScellular is responsible for device delivery and data service. StreamWIDE is responsible for Team on the Run solution delivery and SaaS service.

b. Project coordination

Team on the Run project coordination will be performed by StreamWIDE and UScellular teams. A limited duration trial of the solution can be coordinated with customer if needed. All StreamWIDE project coordination is done remotely for accounts 500 users or less.

c. Installation and Testing process

Based on the identified user list and use cases Team on the Run team will support the initial setup to maximize the value captured by customer:

- Creation of users
- Configuration of user rights and roles
- Process template creation (1 template and 1-hour consultation included)
- Activation of devices
- Assistance with implementation questions

d. Client Infrastructure and support assessment process

Our dedicated support team will work with you to understand your infrastructure and assess your support needs. We will create a comprehensive support plan to meet those needs.

e. End user Acceptance process

Once installation and deployment are complete StreamWIDE will conduct training and in this session the acceptance is reached.

At this point, customer can reach Team on the Run support.

f. Approach to maintenance and support

StreamWIDE customers have access to 24/7 email support. Contact button on the client app to reach support team.

g. Initial and Ongoing Training provided

Team on the Run training is performed by StreamWIDE team product expert and typically delivered remotely. The training is centered on the customer use cases.

Ongoing questions on the product after initial training can be addressed by Team on the Run support team.

h. On-going support and enhancement over the life of the agreement

Team on the Run account manager assigned to customer is the responsible for customer satisfaction and the single point of contact for commercial requests such as additional licenses or plan changes.

Team on the Run is an active product and it continuously evolves. Feature enhancements are pushed via the SaaS platform to customers. Our marketing team communicates the enhancements and our

support and account managers are ready to answer any questions. Typically, enhancements in existing features are backward compatible so minimum impact is expected on customers already using the functions.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution

Team on the Run standard implementation includes the following services provided by StreamWIDE:

- Implementation services / My Business activation
 - o Initial configuration and creation of users on SaaS solution
 - o Installation support of mobile client app on customer devices
 - o Training session
- Team on the Run SaaS Service
- Team on the Run Support service

Additional consulting services can be ordered as needed.

- b. Experience and qualifications of partners and subcontractors
StreamWIDE implementation and support engineers are full- time employees and specialize in the Team on the Run product. Internal processes are in place that allow escalation to product and development managers if questions or issues arise.
- c. Description of Additional Integration and Consulting Services provided
Additionally, StreamWIDE can provide consultation services for:
- Special Integration services (API integration with external systems).



StreamWIDE

Security - Internal Policy

Product Document



StreamWIDE Security 1.0

Product Document

Document History:

Version #	Date	Edition cause	Author(s)
1.0	2019-Feb-10	First release	Cosmin CECANAU

Document Approvals:

Version #	Date	Name	Visa
1.0	2019-Feb-10	Cosmin CECANAU	Security Manager

TABLE OF CONTENTS

1. Policy brief & purpose	4
2. Scope	5
3. Policy elements	6
3.1. Confidential data	6
3.2. Protect personal and company devices	6
3.3. Keep emails safe	7
3.4. Manage passwords properly	7
3.5. Transfer data securely	7
3.6. Additional measures	8
3.7. Social media policy	8
3.8. Internet usage policy	9
3.9. Remote employees	9
4. Disciplinary Action	11
4.1. Take security seriously	11



1. Policy brief & purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

It refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	4/11



2. Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	5/11

3. Policy elements

3.1. Confidential data

Confidential data is secret and valuable.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive customer data.)
- Constitute the backbone of our business, giving us a competitive advantage

Employees will unavoidably receive and handle personal and private information about clients, partners and our company. We want to make sure that this information is well-protected.

Our company most important confidential assets are:

- In-house developed software
- Unpublished financial information
- Data of Customers/Partners/Vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Each employee is obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

3.2. Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only. We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	6/11

When new hires receive company-issued equipment they will receive instructions for:

- *Disk encryption setup*
- *Password management tool setup*
- *Installation of antivirus/ anti-malware software*

They should follow instructions to protect their devices and refer to our *Internal Support Engineers/ Network Engineers* if they have any questions.

3.3. Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Do not open emails when sender is unknown. Even when sender is known, it may be a fake origin (spoofing). In such cases be cautious if the title or content looks unusual for such sender.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they can refer to our *IT Support department*.

3.4. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every three months.

3.5. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our *Internal Support Engineers* for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	7/11

connection.

- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our *IT Specialists/ Network Engineers* need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our *IT Specialists/ Network Engineers* must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Internal Support engineers are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

3.6. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to *HR/ IT Department*.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy (as described in the corresponding chapters below).

Our *Internal Support Engineers/ Network Administrators* will:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company does all the efforts to have all physical and digital shields to protect information.

3.7. Social media policy

Social media refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them.

We allow employees to access their personal accounts at work. But, we expect them to act responsibly and ensure their productivity isn't affected. Using social media excessively while at work can reduce efficiency and concentration. Whether employees are using their accounts for business or personal purposes, they may easily get sidetracked by the vast amount of available content.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	8/11

We advise our employees to:

- Use their common sense. If employees neglect their job duties to spend time on social media, their decline in productivity will show on their performance reviews.
- Ensure others know that personal account or statements don't represent our company. Employees shouldn't state or imply that their personal opinions and content are authorized or endorsed by our company. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
- Avoid sharing intellectual property like trademarks on a personal account without approval. Confidentiality policies and laws always apply.
- Avoid any defamatory, offensive or derogatory content. It may be considered as a violation of our company's anti-harassment policy, if directed towards colleagues, clients or partners.

3.8. Internet usage policy

Our employees are advised to use our company's internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor.

3.9. Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	9/11



StreamWIDE Security 1.0

Product Document

accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our *Internal Support Engineers/ IT Administrators*.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 Security - Internal Policy	10/11

4. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary actions up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face Progressive Discipline, even if their behavior hasn't resulted in a security breach.

Our Progressive Discipline policy outlines the steps we will take to address an employee's misconduct.

We recognize that people make mistakes and our employees may not always follow our policies closely. We want to give our employees a chance to correct their behavior when possible and assist them in the process. We also want to ensure that serious offenses are thoroughly investigated and dealt with.

This policy applies to all our employees.

Our disciplinary process has six steps of increasing strictness. These steps are:

- Verbal warning
- Informal meeting with supervisor
- Formal reprimand
- Formal disciplinary meeting
- Penalties
- Termination

4.1. Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.



StreamWIDE Security 1.0



STREAMWIDE Information Security Management System

Product Document



StreamWIDE Security 1.0

Product Document

Document History:

Version #	Date	Edition cause	Author(s)
1.0	2020-Feb-10	First release	Cosmin CECANAU

Document Approvals:

Version #	Date	Name	Visa
1.0	2020-Feb-10	Zakaria NADHIR	CTO

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	2/19



StreamWIDE Security 1.0

Product Document

TABLE OF CONTENTS

1.General view	4
2.Direction	5
3.Scope	6
4.Top Management Leadership and Commitment	7
5.Internal Audit and Employees Continuous Mindset Growth	8
6.Infrastructure Continuous Security	9
7.Software Continuous Security	10
7.1.IDE: IntelliJ IDEA SonarLint	10
7.2.Version Control System: Subversion	11
7.3.Manual Security Check	12
7.3.1.Team Leader Review	12
7.3.2.Dedicated Testing Team	12
7.4.Automated Security Scan	12
7.4.1.Sonar Qube	14
7.4.2.Lint	16
7.4.3.Mobile Security Framework (MobSF)	18

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	3/19



StreamWIDE Security 1.0

Product Document

1. General view

An Information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data.

The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	4/19



StreamWIDE Security 1.0

Product Document

2. Direction

StreamWIDE guidelines and provisions for establishing, implementing, maintaining and continually improving the internal ISMS are following **ISO/IEC 27001:2013** recommendations.

ISO 27001 is a specification for creating an ISMS. It does not mandate specific actions, but includes suggestions for documentation, internal audits, continual improvement, and corrective and preventive action.

StreamWIDE Top Management and Security Team are doing best efforts to follow and adapt the standard recommendations with the goal of keeping our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	5/19



StreamWIDE Security 1.0

Product Document

3. Scope

The document offers a high level overview over the *concrete and provable* actions taken by the Company in order to ensure continuous security improvements

- Top Management Leadership and Commitment
- Internal Audits and Employees Continuous Mindset Growth
- Infrastructure Continuous Security
- Software Continuous Security

External references should be additionally provided:

- [SW_InternalSecurityPolicy](#) - Internal Security Policy document
- [SW_0G_BusinessContinuityPlan](#) - Business Continuity Plan document

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	6/19



4. Top Management Leadership and Commitment

Top Management assume their responsibilities for Information Security/Business Continuity and ensure all required actions are part of company strategy.

Business Continuity Process

The STREAMWIDE Business Continuity Plan aims to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters include all the cases where business is not able to occur under normal conditions.

The main objectives of the plan are:

- Facilitate effective decision-making to ensure that StreamWIDE operations are restored in timely manner in case of service interruption
- Protect essential facilities, equipment, vital records and other assets
- Protect the well-being of StreamWIDE's employees and customers
- Minimize loss of revenue/customers
- Maintain public image and reputation
- Minimize loss of data
- Minimize the critical decisions to be made in a time of crisis
- Identify teams which would need to respond to a crisis

The process is described in [sw_0G_BusinessContinuityPlan](#) document.

Management follow up and review

The main company security objectives are reviewed each week during the official Masterplan Status Meeting with Product Managers.

Additionally, relevant KPIs on [Software Security](#) are sent weekly for management reviews.

Among other information they include the number of vulnerabilities and bugs reported when scanning the code using tools recommended by OWASP.

Security Events Reporting

Since executives are the ones who have the most influence in an organization, Security objectives or Measures for Crisis management are always part of Top Management communication.

Internal Security Policy

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, Top Management has implemented a number of security measures presented by [SW_InternalSecurityPolicy](#).

With this policy, STREAMWIDE ensures that we gather, store and handle data fairly, transparently and with respect towards individual rights.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	7/19



5. Internal Audit and Employees Continuous Mindset Growth

STREAMWIDE Internal security audits are oriented to people awareness, processes, policies and infrastructure hardening.

Software Audit is treated as independent process using automated solutions according to Continuous Security guidelines.

Auditors

Internal audits are performed and coordinated by employees with **important company history and relevant experience in various domains (development, linux administration, team lead, team management)**.

Cosmin CECANAU

Position: Product Manager Installer Team, Manager of Romania Security department, certified for Internal Auditor iso 27001/2013 international recognition

Activity: Coordinates the security department activities based on priorities (implementations, standards appliance, trainings)

Studied: The Faculty of Automatic Control and Computer Science (Polytechnic University of Bucharest);
In StreamWIDE since 2006 ,

Thomas BOUTON

Position: Chief Software Architect / Chief Security Officer

Activity: Coordinates company security activities according to customers needs, creates and validates software architectures.

Studied : Ecole Nationale Supérieure des Télécommunications de Paris
In StreamWIDE since 2001,

Cristian RADU

Position: Product Manager StreamWIDE Messaging System & SmartMS Backend

Activity: Collaborates with the security department bringing concrete lessons learned, real usecases and needs from Messaging Product life history & SmartMS backend new challenges.

Studied: The Faculty of Electronics Telecommunications and Information Technology (Polytechnic University Bucharest);
In StreamWIDE since 2008,

Scheduling

The frequency for Internal auditing a StreamWIDE Subsidiary depends on the activities performed and the number of employees. It is done once or twice per year.

Normally the audit is done on-site. But depending on situation can be done remotely. The audit lasts *3 to 5 days*.

Reporting and Follow Up

The internal Audit is finished by a "conclusions meeting" with the local management. Also an email with conclusions and action plan is sent to the Top Management.

The actions will be followed up weekly as explained in the "Top Management Leadership and Commitment" chapter.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	8/19



6. Infrastructure Continuous Security

Identifying vulnerabilities and gaining visibility into the number of smart devices and their role within the infrastructure can help reduce the risk of a successful cyberattack.

It's important to keep a detailed inventory of all IoTs, constantly check for new security updates that address known vulnerabilities, and maintain them on a segregated network that's completely isolated from other critical systems.

Actions for increasing the security of the company infrastructure are decided during regular audits or during technical workshops.

Some element are listed below, but for confidentiality reasons there are no concrete technical descriptions for the actions taken.

Network Topology

Keeping up-to-date and understanding our own topological structure of the network, physically or logically it is a key requirement for our administrators.

Network segmentation

Network segmentation is a mandatory element for ensuring security.

VPN

VPN solution having high level encryption and Multi Factor Authentication is a mandatory element to ensure safe remote connections.

Firewall

Firewall is one of the cornerstones of any network security strategy so it is mandatory to use a performant solution.

Backup

Ensuring backups gives fast recovery in case of data loss.

Wifi

Wifi Security hardening has also been taken in consideration.

External Scan

External scanning is regularly notifying the administrators about potential flaws of our network.

Intrusion Detection

Intrusion detection systems or traps are offering precious time in preventing a cyberattack.

Secure Communication

Replacing deprecated protocols with latest secure protocols is also a continuous process.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	9/19



StreamWIDE Security 1.0

Product Document

7. Software Continuous Security

StreamWIDE target is to align all proprietary software modules/applications to the newest recommendations regarding Continuous Security.

This chapter explains the process used to ensure Continuous Security for an Android Mobile Application belonging to StreamWIDE software suite.

The rest of **STREAMWIDE** software modules/applications implement **PARTIALLY** this model at this time.

 Code inspection starts from the very first code view due to specialized IDE.

 A popular version control system is used to ensure that all the changes are tracked or can be reverted.

 Manual checking and testing is done by Team Leaders and dedicated Testing Team.

 Automated scan is done by popular and powerful tools on daily, on demand or on commit basis in order to help the team with comprehensive security reports or regressions alerts.

7.1. IDE: IntelliJ IDEA SonarLint

StreamWIDE Android team uses **IntelliJ IDEA with SonarLint plugin** for code development.

IntelliJ IDEA is a Java integrated development environment (IDE) for developing computer software.

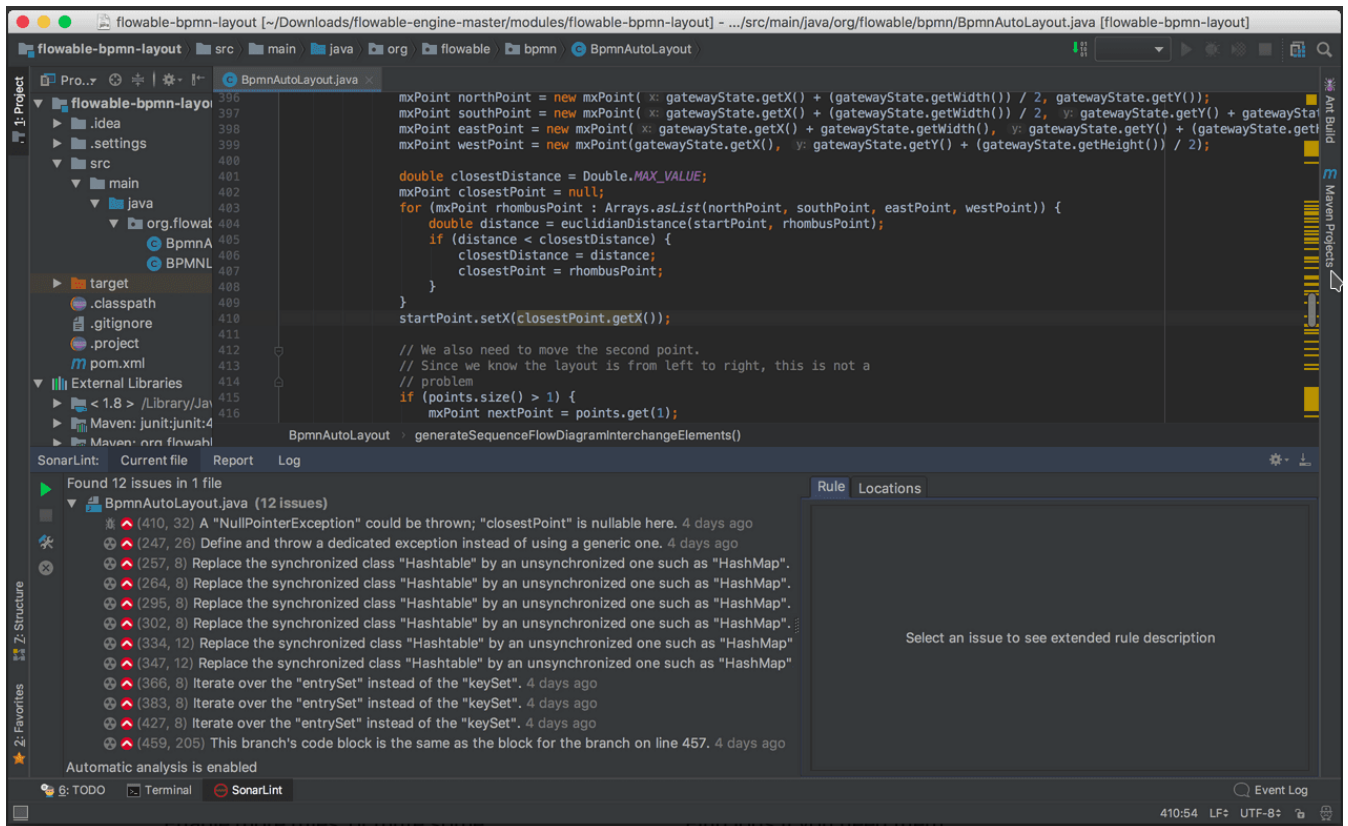
SonarLint is an IDE extension that helps detecting and fixing quality issues as code is being written. Like a spell checker, SonarLint squiggles flaws so that they can be fixed before committing code.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	10/19



StreamWIDE Security 1.0

Product Document



7.2. Version Control System: Subversion

Android Team uses **Subversion** in order to keep the track of every code modification.

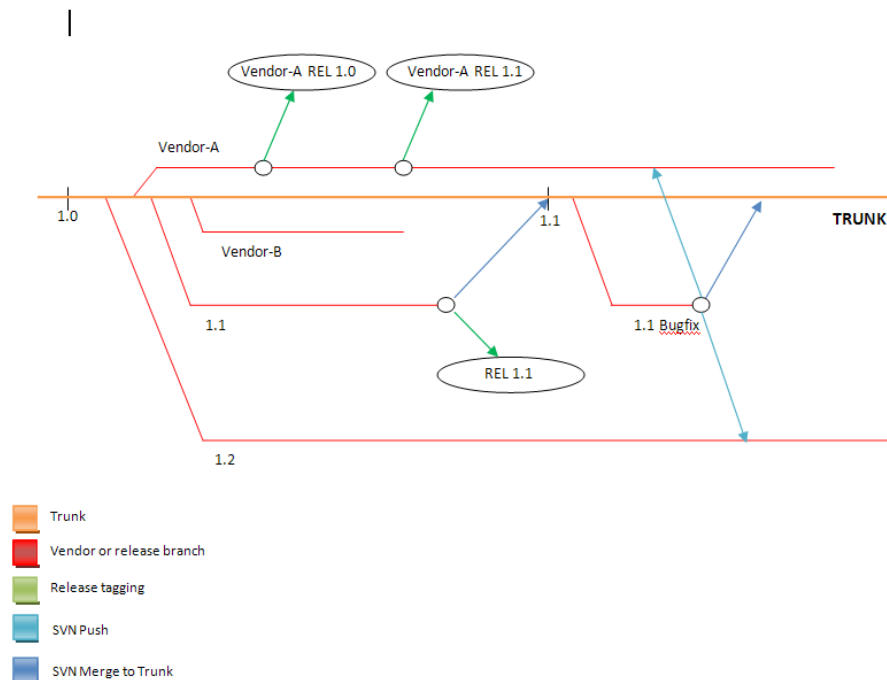


Subversion is a free/open source version control system. That is, Subversion manages files and directories, and the changes made to them, over time.

This allows us to recover older versions of the data or examine the history of how your data changed.

Android Team is using the recommended mechanism with trunk & branches.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	11/19



7.3. Manual Security Check

7.3.1. Team Leader Review

The Android development team distribution ensures a tight control for every piece of code which reaches the repository.

The team is split in small subteams lead by Team Leaders.

Any new code is reviewed by at least a Team Leader before being merged to the main Subversion branch.

Critical code is also reviewed by Product Manager.

7.3.2. Dedicated Testing Team

A dedicated testing team is in-charged of manual testing every new minor and major release.

Although the tests are mostly functional, security fixes receive a special attention and important time allocated.

7.4. Automated Security Scan

A complex mechanism is designed to ensure security scanning on a regular base or on each merge in the main branch (depending on the configuration).

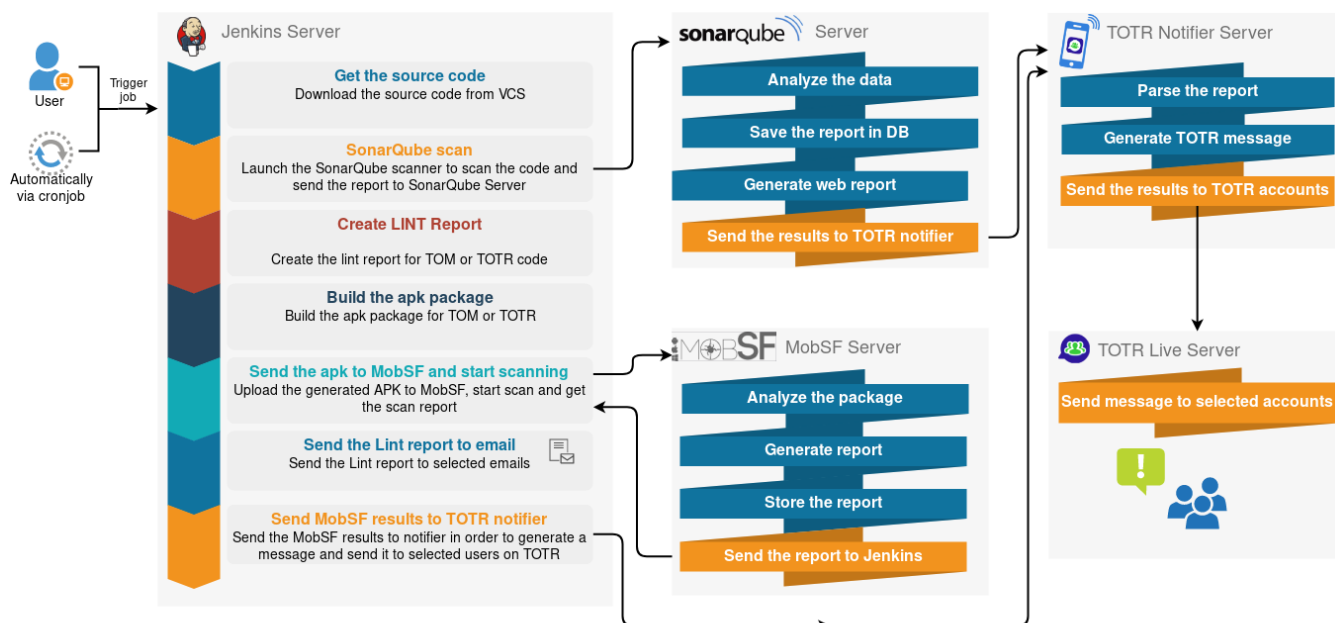
Powerful tools like Jenkins, SonarQube, Lint or MobSF are combined to ensure a complete security verification as it is presented in the diagram below.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	12/19



StreamWIDE Security 1.0

Product Document



© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	13/19

7.4.1. Sonar Qube



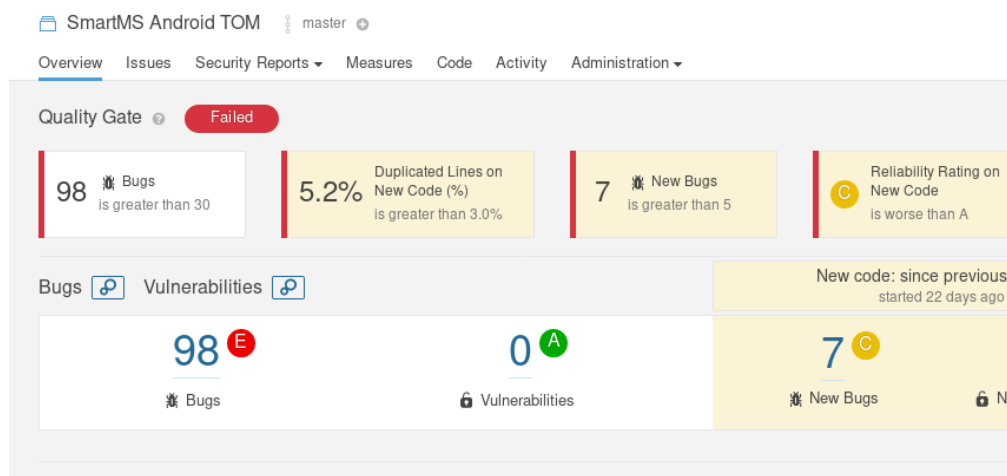
The OWASP SonarQube project aims to provide open source Static Application Security Testing (SAST) using the existing open source solutions.

SonarQube is one of the world's most popular continuous code quality tools and it's actively used by many developers and companies.

SonarQube has helped Android team to improve drastically the quality of the software.

Daily reports are showing the potential vulnerabilities and issues helping the team to understand the threats and principles for good quality and security.

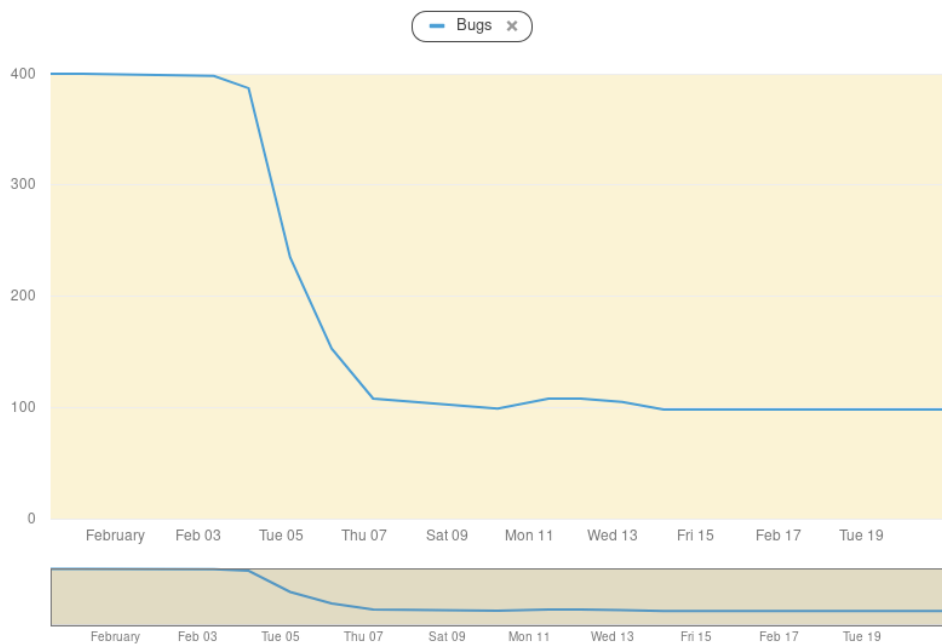
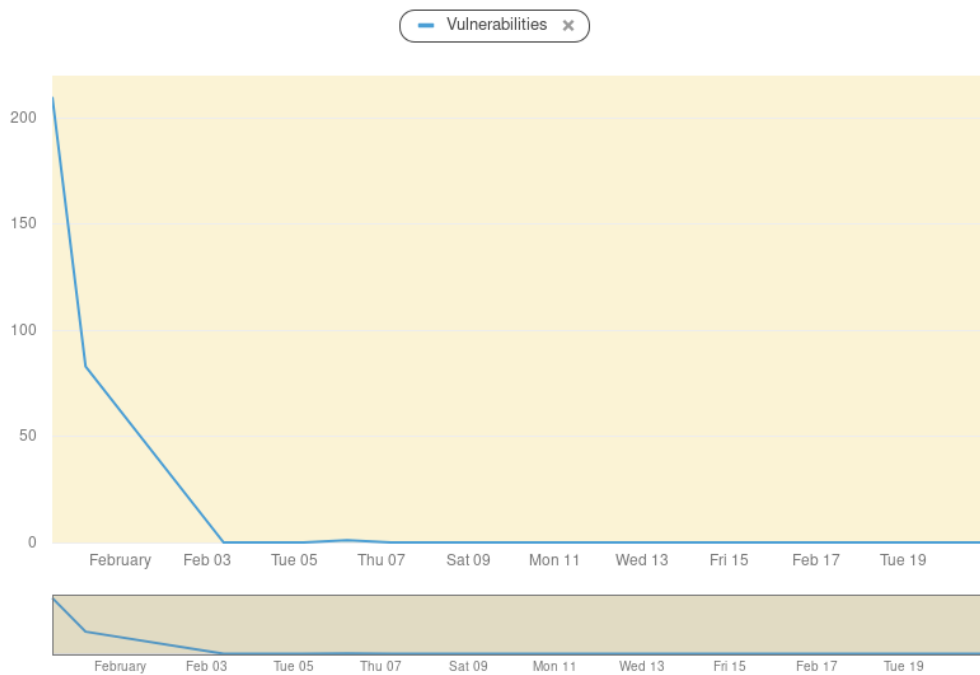
The reports below are taken at 22 Feb 2019. By this date the team has done big efforts to decrease to 0 the number of vulnerabilities and it is concentrating right now to decrease also the number of potential bugs.





StreamWIDE Security 1.0

Product Document



© StreamWIDE All rights reserved	Author: Cosmin CECANAU StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	Date: 2019-Feb-10 15/19



StreamWIDE Security 1.0

Product Document

7.4.2. Lint

Android build system provides a lot of tools to optimize the code, find potential issues, improve performance, etc. One of the tool it supports is Lint. Lint is a tool which analyzes the source code and flags potential bugs and errors during the build.

Daily reports are showing the potential vulnerabilities and issues helping the team to understand the threats and principles for good quality and security.

The reports below are taken at 22 Feb 2019. By this date the team has done big efforts to decrease the number of vulnerability notices and it is concentrating right now to decrease also the number of potential issues..

Overview

Correctness	
4	! MissingRegistered : Missing registered class
9	! ApplySharedPref : Use apply() on SharedPreferences
1	! PrivateApi : Using Private APIs
1	! UnusedAttribute : Attribute unused on older versions
1	! BatteryLife : Battery Life Issues
5	! InflateParams : Layout Inflation without a Parent
1	! NewerVersionAvailable : Newer Library Versions Available
5	! RestrictedApi : Restricted API
54	! SwitchIntDef : Missing @IntDef in Switch
Correctness:Messages	
3	! Typos : Spelling error
Security	
1	! BadHostnameVerifier : Insecure HostnameVerifier
3	! HardwareIds : Hardware Id Usage
1	! SetJavaScriptEnabled : Using setJavaScriptEnabled

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	16/19



StreamWIDE Security 1.0

Product Document

Performance

2	⚠ DrawAllocation : Memory allocations within drawing code
2	⚠ WakelockTimeout : Using wakeLock without timeout
6	⚠ ObsoleteLayoutParam : Obsolete layout params
73	⚠ ObsoleteSdkInt : Obsolete SDK_INT Version Check
3	⚠ StaticFieldLeak : Static Field Leaks
1	⚠ VectorPath : Long vector paths
4	⚠ UseSparseArrays : HashMap can be replaced with SparseArray
1	⚠ DisableBaselineAlignment : Missing baselineAligned attribute
2	⚠ InefficientWeight : Inefficient layout weight
6	⚠ Overdraw : Overdraw: Painting regions more than once
82	⚠ UnusedResources : Unused resources
5	⚠ UselessParent : Useless parent layout
35	⚠ UnusedIds : Unused id
1	⚠ UnusedNamespace : Unused namespace

Usability:Typography

1	⚠ TypographyQuotes : Straight quotes can be replaced with curvy quotes

7.4.3. Mobile Security Framework (MobSF)

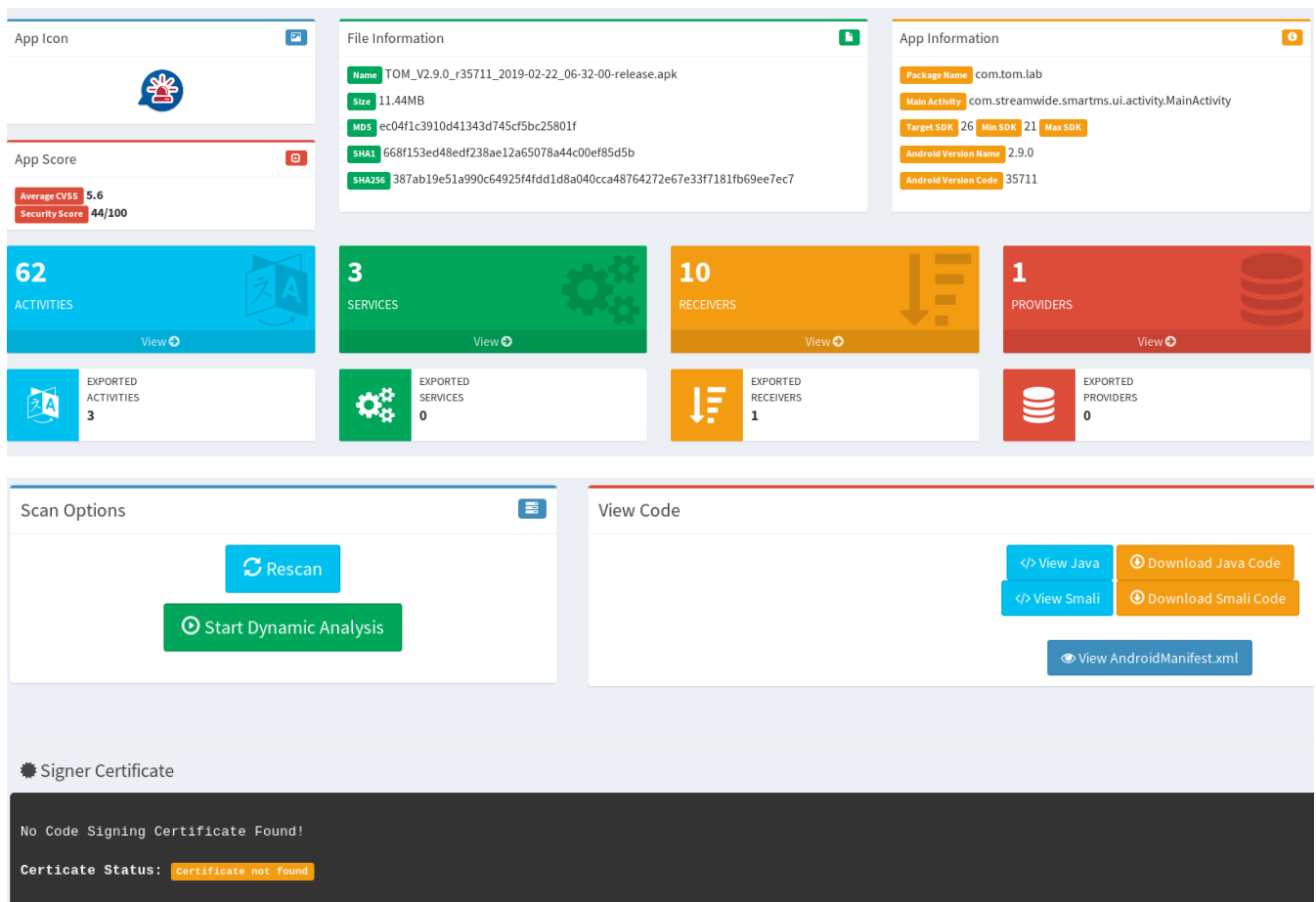


Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing framework capable of performing static, dynamic and malware analysis. It can be used for effective and fast security analysis of Android, iOS and Windows mobile applications and support both binaries (APK, IPA & APPX) and zipped source code.

MobSF can do dynamic application testing at runtime for Android apps.

This option it is used by Android Team on a regular basis to investigate the potential security issues of the apk.

Below are some examples of report taken on 22 Feb 2019.



The screenshot displays the MobSF web interface with the following sections:

- App Icon:** Shows the application icon for 'com.tom.lab'.
- App Score:** Displays an Average CVSS of 5.6 and a Security Score of 44/100.
- File Information:**
 - Name: TOM_V2.9.0_r35711_2019-02-22_06-32-00-release.apk
 - Size: 11.44MB
 - MD5: ec04f1c3910d41343d745cf5bc25801f
 - SHA1: 668f153ed48edf238ae12a65078a44c00ef85d5b
 - SHA256: 387ab19e51a990c64925f4fdd1d8a040cca48764272e67e33f7181fb69ee7ec7
- App Information:**
 - Package Name: com.tom.lab
 - Main Activity: com.streamwide.smartms.ui.activity.MainActivity
 - Target SDK: 26, Min SDK: 21, Max SDK: 28
 - Android Version Name: 2.9.0
 - Android Version Code: 35711
- Summary Cards:**
 - 62 ACTIVITIES (View)
 - 3 SERVICES (View)
 - 10 RECEIVERS (View)
 - 1 PROVIDERS (View)
- Exported Data:**
 - EXPORTED ACTIVITIES: 3
 - EXPORTED SERVICES: 0
 - EXPORTED RECEIVERS: 1
 - EXPORTED PROVIDERS: 0
- Scan Options:**
 - Rescan button
 - Start Dynamic Analysis button
- View Code:**
 - View Java / Download Java Code
 - View Smali / Download Smali Code
 - View AndroidManifest.xml
- Signer Certificate:**
 - No Code Signing Certificate Found!
 - Certificate Status: Certificate not found



StreamWIDE Security 1.0

Product Document

Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	dangerous	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and networks.

© StreamWIDE	Author: Cosmin CECANAU	Date: 2019-Feb-10
All rights reserved	StreamWIDE Security 1.0 STREAMWIDE Information Security Management System	19/19



StreamWIDE

Warning Procedure for Internal and External Customers

Operational Guideline

Document History:

Version #	Date	Edition cause	Author(s)
1.0	16/04/2012	First Release	Victorita ANECHITEI

Document Approvals:

Version #	Date	Name	Visa
1.0	16/04/2012	Zakaria NADHIR	ZN

Storage :

PDF Document	Document Sources
Alfresco:\Quality\05.Process&Procedures\Technical Support	Alfresco:\Quality\04.Sources\Technical Support

TABLE OF CONTENTS

1.	Introduction	4
1.1.	Purpose	4
1.2.	Scope	4
1.3.	Definitions and Acronyms	4
1.4.	Role	4
2.	Inputs.....	4
3.	Activities	4
3.1.	On the CTO's side	4
3.1.1.	Gathering and analyzing information	4
3.1.2.	E-mail to Support and Quality	4
3.2.	On the Support Manager's side.....	5
3.2.1.	Warning e-mail internally	5
3.2.1.	Warning e-mail for customers.....	5
3.3.	On the Customer's side	5

1. Introduction

1.1. Purpose

This document describes the policy implemented by StreamWide to insure a proactive support attitude in the case of redundant critical issues and a better circuit of pertinent information inside StreamWide regarding service impacting issues.

1.2. Scope

This procedure relates to the full range of company activities, mainly to issues regarding software development, delivery and technical support.

1.3. Definitions and Acronyms

CTO – Chief Technology Officer

1.4. Role

Under this procedure the CTO is in charge of selecting the pertinent warnings to be sent internally and to the customers.

2. Inputs

Feedback from support, delivery and product teams on critical issues.

3. Activities

3.1. On the CTO's side

3.1.1. Gathering and analyzing information

Every week, the CTO (Zakaria Nadhir) will analyze the main problematic issues that will appear on the customers platforms based on feedback from delivery, support and product teams. He will decide whether there is a real need to send a warning internally and to the customers. The CTO is in charge of selecting the most risky issues among the ones that have been escalated in the given period of time.

3.1.2. E-mail to Support and Quality

As often as needed, the CTO will send an e-mail to the Support and Quality departments to inform them of the main problems that have occurred during the given period and that might risk reappearing on other platforms.

The e-mail sent by the CTO will include for each issue raised:

- a description of the issue

© StreamWIDE	Author: vanechitei	
All rights reserved	sw_OG_Warning Procedure for Internal and External Customers10	4/5

- which are the versions of products that might be impacted
- which are the exceptions to be taken into account when sending the warning e-mails to the customers.

3.2. On the Support Manager's side

3.2.1. Warning e-mail internally

Based on the CTO's e-mail, the support manager must issue a warning e-mail internally with the following list of users, all in Cci:

- support team
- delivery team
- product teams (PMs)
- sales.

Each support engineer has under his direct supervision a list of customers. (See **StreamWIDE Support - Internal Handover Process**, on **Alfreco:\Quality\05.Process&Procedures\Technical Support**). Each of them will have to check in the CRM to see which of his/her customers/platforms might be impacted by the issues raised in the Support Managers' e-mail. If any identified customers, they will inform the Support Manager about it.

This task is considered as level 1 Task, on the support list of tasks.

3.2.1. Warning e-mail for customers

In three days time after having received the CTO's e-mail, the Support Manager will have to send a warning e-mail to all customers concerned by the issues. A special e-mail template will be used for the warning and each customer will receive an individual e-mail (no Cci). Each sent e-mail will be accompanied by the opening of a ticket in the ticketing tool.

- Prior to issuing a warning to customer, Support should inform sales that a warning will be issued. If sales do not answer within 2 workdays, warning is issued, if they ask not to issue or to delay the warning for commercial reasons, they take the responsibility if any problem related to the warning occurs on the platforms. Information to sales should include the solutions they can propose to their customers.
- When the warning is issued to a customer it should contain also a solution/recommendation. A warning with no solution proposed would generate high customer anxiety and may trigger wrong reactions.

3.3. On the Customer's side

Based on the raised issue, the customer should get in touch with his Sales contact inside of StreamWide to be informed of the options that we might propose to fix the issue (e.g. : ask for an upgrade, a fix etc.)

If the customer doesn't reply after two reminders, the Support department is allowed to close the ticket and consider the warning closed.

© StreamWIDE	Author: vanechitei	
All rights reserved	sw_OG_Warning Procedure for Internal and External Customers10	5/5

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory F: Mobile Data Collection/Mobile Forms

Subcategory I: Public Safety Systems

Subcategory M: Enterprise Messaging

Client Company name:

Tennessee Trash Service Solution

Client name of contact:

Steve Turner

Client contact title:

Owner

Client is a daily user, occasional user, etc.:

Daily

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Kevin Dylla no later than Friday, November 6th.

Thank you for your assistance in this process.

1. For what services do you use USCC's product, and how long have you been USCC's customer?

Vendor used: Team On The Run by StreamWIDE

Steve Turner, Owner

Cell: 865-740-7771

stevet@tntrashservice.com

Licenses: 68 Team on The Run licenses

Tennessee Trash Service is a residential & commercial garbage removal company located in Knoxville, Tennessee. We were interested in a new fleet solution for drivers covering a 100-mile radius of Knoxville with different routes every day. We were using push to talk on basic phones to dispatch the entire fleet, which was inefficient, noisy and chaotic by giving verbal turn by turn directions and also trying to determine drivers' locations to pick up misses. Fleet solution would need to refresh data more frequently to have more accurate speed alerts to enforce safety policies. Lastly, we wanted to see all of the routes in the fleet management portal to ensure route optimization.

2. Would you recommend USCC to other customers? Why?

Yes, because the product is easy to use, saves time and saves money.

3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?

Met milestones

4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?

5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?

Replacing basic driver phones with ruggedized smart phones with Team on the Run for push to talk capability helped making the dispatch process easier & more productive by pushing out Google Map links to drivers for direction, drivers sending pictures/videos from the field, group messaging reducing the chatter in dispatch. MaaS360 locked down the driver smartphones only allowing access to phone calls, Team on the Run, Weather and Google Maps.

6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?

N/A

7. Is there anything else you think we should know about working with USCC or using USCC's products and services?

N/A

8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?

None

Appendix Y

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory N: Secure LAN Access

Private Tunneler Virtual Private Network



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
[Private Tunneled Virtual Private Network](#)
- b. General Application Area
[Subcategory N: Secure Lan Access](#)
- c. General capabilities provided
[Encrypted traffic, Private Static IP address assignment, GRE over IPSEC tunnels.](#)
- d. Expected impact on cost/performance/functionality, etc.
[Enhanced Security and control](#)
- e. Subcontractors/partners involved in delivering service
[Affirmed, Nokia, Ericsson, Cisco, Palo Alto](#)
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
[No](#)

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
[AES \(Advanced Encryption Standard\) is the strongest encryption algorithm available used with IPSEC tunnels. Geographically redundant Aggregation Service Routers \(ASR\) ensure high availability and reliability.](#)
- b. Applicability to government needs
[Secure encrypted traffic, Private Static IP address assignment, GRE over IPSEC tunnels, high availability and redundancy.](#)
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
[UScellular currently has 30+ GRE over IPSEC Virtualized Private Networks setup with various business and government agencies.](#)

[References:](#)
[WEC Energy Group](#)
[Steve Liegl, Director Infrastructure and Operations](#)
[See Attachment Q](#)

- d. Overall interoperability of turnkey system for government use
UScellular supports a wide range of customization to support interoperability with the infrastructure the government has in place.
- e. Accessories available for turnkey offering
None.
- f. Thoroughness of the vetting process used to select partners
UScellular uses the RFP process to thoroughly evaluate competing vendor solutions against the business needs and objectives. The vendor evaluations include but are not limited to:
 - 1) Alignment with UScellular's system architecture philosophy
 - 2) Availability, reliability, scalability, performance, maintainability, and security requirements
 - 3) Vendor's solution maturity and adoption in North America
 - 4) Vendor's financial standing
 - 5) Standards and Regulatory compliance

The vendor solutions are also trialed in a lab prior to being selected.

- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

Lab testing process:

All new components and services provided by the vendor(s) have defined goals captured as use cases. The test cases are defined that trace back to the use cases. To verify and validate that the overall solution achieves its goals without any defects, the test cases are executed against the system in the test lab. The test cases validate the solution both at the component and system integration level. Regression test suite is also executed against the system to verify/validate existing system functionality is free of any new defects. Before going live, similar verification and validation process is executed in the production environment.

Production ATP (Acceptance Test Plan) process:

For ATP Testing, we have standard test cases for all call flows that a particular network component must pass (based on already deployed services). We then work with our vendor (every SoW we do with our vendors to deploy new elements or services has a section that calls out the ATP creation steps, execution steps and that all tests must pass) and our lab teams (ATS/ASEP/lab personnel) to ensure we incorporate any new test cases for a new service that will be deployed. In order to pass, all regression testing must pass 100% and all new test cases must pass 100%. The ATP is run on both Lab and production sites. We also incorporate failover testing to ensure any new element or service works during both any local or geographical failure, using that same ATP. Each ATP is peer reviewed by multiple engineers and teams.

KPIs (Key Performance Indicators):

KPIs are developed to allow monitoring of key network statistics which would indicate a product or service may not be performing or operating as expected. The KPIs are developed during testing and then subsequently monitored and alarmed on by UScellular's National Network Operations Center throughout the life of the service.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
UScellular's Wireless Solutions Architects perform pre-installation coordination between UScellular and the customer.
- b. Project coordination
The Wireless Solutions Architects and Core Service Integration team assign a dedicated resource to each business or government entity who want to setup a virtualized private network.
- c. Installation and Testing process
The Wireless Solutions Architects and Core Service Integration team coordinate the installation, turn up and testing process with the technical resources from the business or government entity.
- d. Client Infrastructure and support assessment process
UScellular's Wireless Solution Architects with support of Engineering to perform assessments.
- e. End user Acceptance process
Technical support team available during user acceptance testing.
- f. Approach to maintenance and support
Dedicated Wireless Solutions Architect.
Dedicated 24x7 National Network Operations Center support.
Specialized Technical Support team to triage customer issues.
Notifications supplied of planned network maintenance (Upgrades, Feature Enhancements) and outages.
- g. Initial and Ongoing Training provided
UScellular offers training to customers at no additional charge.
- h. On-going support and enhancement over the life of the agreement
UScellular continually enhances its network and services to ensure the utmost reliability and availability for its customers. Customer focused support is provided for the life of the contract.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
 - Dedicated Wireless Solutions Architects for the account.
 - Dedicated Technical Customer Service IoT support queue.
 - Dedicated 24x7 emergency support via the National Network Operations Center.
- b. Experience and qualifications of partners and subcontractors
 - As part of our RFP activities, we carefully review the qualifications and capabilities of potential vendors through the information they provide and confirm these qualities/capabilities through reference calls and other available benchmarking data.
- c. Description of Additional Integration and Consulting Services provided
 - Depending on customer's chosen solution, additional consulting and integration services are available.

Appendix Z

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory N: Secure LAN Access

CyberReef



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
 - 1. Secure Bandwidth Manager – Mobile data insight, control & security
 - 2. Private NetworkingPlus – Provides protection from cyberattacks on Mobile IoT and M2M devices
 - 3. UptimeEnterprise – business continuity – failover to cellular
- b. General Application Area
Subcategory N: Secure LAN Access
- c. General capabilities provided
CyberReef Solutions will leverage its patented secure cloud-based solution to provide private networking and website filtering for all states participating in the NASPO ValuePoint agreement.
- d. Expected impact on cost/performance/functionality, etc.
Average savings 50-70% on mobile data usage.
- e. Subcontractors/partners involved in delivering service
US Cellular, Verizon, AT&T, and Sprint
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes. Please see attached.



CyberReef Managed
Services Terms and C

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
 - Cost Management
We help by giving you daily visibility and control of all mobile data usage. Easily control data costs with the click of a button.
 - Mobile Internet Use Policy
We eliminate data and compliance risks by extending the safety of your in-office wireless Internet use policy to the mobile environment.
 - Security
Protect all enterprise mobile devices by deploying a secure private mobile network. No device apps required.

- b. Applicability to government needs
Current customers use our solution to secure smartphones, tablets, IoT devices, cellular hotspots, routers and wearable devices. Governments utilize our solutions to manage costs, manage mobile internet use policies and manage security.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
Our solution has been sold into the commercial and educational marketplace since 2013.

Key customers include Fortune 1000 companies and K-12 schools. We have deployed 400,000+ lines
- d. Overall interoperability of turnkey system for government use
Our solution works on all modem, tablet, smartphone manufacturers.
- e. Accessories available for turnkey offering
N/A
- f. Thoroughness of the vetting process used to select partners
Nearly half of our staff is assigned to R&D and have experience commercializing our solution with very large customers and mobile carriers.

Over the last 2 years, we have worked with Fourteen IP, Carl's Jr./Hardees, ServiceNow, Dover Lifts, Texas Board of Education, California Board of Education, Stockton Unified School Districts and more to deploy our custom services.

We will leverage our experience to ensure flawless deployment of our services.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
Our patented architecture/solution allows us to start initial proof-of-concept of our secure services within a month of contract signing.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
Our project team will meet with you to create an in-depth project plan to launch this solution with the state or municipality.
- b. Project coordination
CyberReef Sales Manager (project manager) and engineer. Also, carrier sales manager and engineer.

c. Installation and Testing process

We will create an implementation flow chart as part of the project coordination meeting that will include all steps of the installation and testing process. This will be managed, implemented and tested by CyberReef in conjunction with UScellular.

d. Client Infrastructure and support assessment process

Our dedicated support team will work with you to understand your infrastructure and assess your support needs. We will create a comprehensive support plan to meet those needs.

e. End user Acceptance process

The End user Acceptance process will be defined in the implementation and testing flow chart during the pre-installation coordination meeting.

f. Approach to maintenance and support

CyberReef's normal support hours are 7AM to 8 PM Central Time Zone. For any planned shutdown of any private network resource, CyberReef (CRS) customers will be notified via e-mail at least 24 hours in advance.

g. Initial and Ongoing Training provided

Portal training – Engineering tier 1 support – Customer support as described in critical path.

h. On-going support and enhancement over the life of the agreement

Reporting Procedure for on-going support:

- For failures with any of CyberReef Solutions services during non-business hours, the automated operator should be contacted at 251-279-0749 please leave voicemail. Your voicemail will be forwarded to the CyberReef Tech team. Also, you can submit a request at <https://www.cyberreefsolutions.com/cyberreef-service-request-form/> which will create a ticket for the tech team. Someone will contact you accordingly
- Please see below our definitions of Call-in Classifications.
 - Critical – Network/Server or critical use Modem – response in an hour or less
 - Major – M2M/IOT device, Smartphone or Tablet connection issue with non-critical equipment – 12-24 hours
 - Minor – Data usage report or general information questions – 24 hours
- If after hours, Non-critical reported problems, (Major or Minor) will be handled the next business day.

After Hours Support Policy

- CyberReef Solutions is committed to making available critical private network and bandwidth management server resources to our customers 24/7. Our team will provide on-call support coverage in the event of unexpected failure or significant problems with critical resources during non-business hours. For a critical issues, support will be available 24/7.
- Resolution of any problem during non-business hours may be dependent upon the nature of the problem and the availability of resources or service and parts from third party vendors. CRS will assess a reported problem and determine a reasonable resolution plan based upon the severity of the problem and resources required. CRS will work to resolve the problem as quickly as possible. For a problem that requires more than four hours to resolve, a status message will be forwarded to our private network customer's point of contact.

4 - Service Factors:

- a. Description of related services included in Turnkey Solution
For state/federal commercialization

Commercialization of our services for state/federal government will not be problematic. We will hire skilled resources in contracts, program management and requirements to build government programs competency.

Competitive Landscape

Our top competitors include Wandera and Asavie. Wandera has a client-based solution for smartphones and tablets but has no solution for IoT devices. Asavie is located in Ireland and has a similar solution to CyberReef, but only our solution is patented and located in the United States.

- b. Experience and qualifications of partners and subcontractors
N/A
- c. Description of Additional Integration and Consulting Services provided
N/A

CyberReef Managed Services Terms & Conditions

1. Definitions:

- 1.1. Authorized Use: The use of the Managed Services that is permitted under these Terms and Conditions.
- 1.2. Legal Notice: Notice given in accordance with the requirements for “Legal Notices” set forth in the “Notices” section below.
- 1.3. Machine-to-Machine or M2M: The transmission of data using the wireless service between wireless devices and computer servers or other machines, or between wireless devices, with limited or no manual intervention or supervision.
- 1.4. Managed Service: The proprietary data control, management, and security services provided by CyberReef.
- 1.5. MTN: Mobile Telephone Number
- 1.6. PRL: Preferred Roaming List

2. Authorized Use and Fraudulent Use:

- 2.1. CyberReef shall provide Managed Service to Customer only under the terms and conditions set forth herein.
- 2.2. Use of wireless service for Remote Medical Monitoring Prohibited: Customer shall not use the Managed Service for remote medical monitoring which, if agreed to by the Parties, would require additional terms and conditions.

3. Acknowledgement:

Customer acknowledges and agrees:

- 3.1. CyberReef may at any time be engaged directly or indirectly, including through or in connection with products and services of its other customers, in soliciting actual or prospective customers for Managed Service or other services, products, or equipment that could be the same as, or similar to, and compete with a Customer Product or Service.
- 3.2. Customer has had the opportunity to independently investigate the Managed Service for use in connection with the Customer Product or Service and the Authorized Use and is not relying on any representation, guarantee, or statement of CyberReef.
- 3.3. CyberReef does not sell hardware but works with partners that do provide equipment to our customers.

4. Purchases by Customer or Authorized Contact(s):

Customer shall identify representatives authorized to purchase Managed Service under these Terms and Conditions and to act on its behalf (“Authorized Contact(s)”) by providing their name(s), telephone number(s), and business and e-mail address (es) in writing to CyberReef. Customer’s initial Authorized

Contact(s) may be identified on the first page of these Terms and Conditions. An Authorized Contact shall have full authority to handle all matters contemplated by the Terms and Conditions or relating to Customer's account(s), unless otherwise specified by Customer in writing to CyberReef. Customer may elect to designate a third party as an Authorized Contact provided it complies with the requirements set forth in the "Customer's Use of Third Parties" section below.

The Authorized contact is deemed to be the signer of this document or his designated replacement if that individual has departed the Customer's Business or has changed jobs within Customer's Business. Additionally, the Customer may list additional approvers. Please add those individuals below:

Printed Name	Title	Contact Email	Contact Phone

5. Customer Billing and Payments:

5.1. Bills: CyberReef bills will be made available on a monthly, quarterly, or yearly basis, and Customer shall pay all fees and charges, including any applicable Taxes and Surcharges. Access fees and feature charges are generally billed in advance, while airtime overage and other usage charges are billed in arrears. Billing cycles vary and may not correspond to calendar months. CyberReef provides billing for third parties, and charges for third party services and applications may be placed on Customer's bill. Customer has the option, at no cost, to block or restrict access to third-party services or applications that may involve a charge being placed on Customer's bill. Customer shall pay all charges attributable to End User use of the Managed Service.

5.2. Payment Terms: Customer shall pay all undisputed charges within 30-days of the date of each bill. Past due amounts shall be, to the extent permitted by the law of the state where Customer's billing address is located, subject to a late payment fee of 1½% per month (18% annually) or \$5 per month, whichever is greater. If payment by check or similar negotiable instrument is returned by a bank for any reason, CyberReef will charge Customer a returned check fee.

5.3. Disputed Charges: In the event of disputed charges, Customer must, as soon as practicable following identification of such dispute, provide written notice to CyberReef, which shall include the date of the bill, disputed amounts, the reason for the dispute, and any supporting documentation. Customer has 180 days from the due date of the bill to notify CyberReef of a disputed charge. The Parties will use their good faith efforts to reconcile any disputed charges within 60 days of the date of notification, after which the Parties may invoke the process set forth in the "Dispute Resolution" section below.

5.4. Failure to Pay: CyberReef may, upon prior written notice to Customer, suspend or terminate Managed Service or deny additional use of the Managed Service due to Customer's failure to either make payment or dispute charges in accordance with the foregoing provisions regardless of any deposit provided by Customer. If CyberReef sends Customer's account to a collection agency, CyberReef may also charge Customer for any fees that CyberReef is charged by the collection agency, if it is permitted by the law of the state where Customer's billing address is located.

6. Taxes, Surcharges and Exemptions:

If any federal, state, local or foreign tax, fee, assessment or other charge is required by law to be collected by CyberReef (each, a "Tax"), or a serving carrier charges Tax on a roaming call, then CyberReef may bill such Tax to Customer, and Customer shall pay such Tax. If CyberReef incurs a tax (other than a net income tax) or other expense to comply with legal or governmental requirements, or other expense to provide or improve service to its customers, and CyberReef bills a surcharge to recover or offset the cost of such expense (a "Surcharge"), then Customer shall pay such Surcharge. Taxes and Surcharges may change from time to time. With respect to any Tax other than a Tax charged by a serving carrier on a roaming call, if Customer provides CyberReef with an exemption certificate in the form provided by law, or with other evidence of exemption acceptable to CyberReef, then that specific Tax will not be collected from Customer. If an exemption applied by CyberReef at Customer's request is found not to apply, then Customer shall upon demand pay CyberReef the uncollected Tax and all related interest, penalties and additions to the Tax. CyberReef shall not issue credits for a Tax that is billed prior to CyberReef's receipt of evidence of exemption.

7. Bankruptcy/Insolvency/Creditworthiness:

Either Party may terminate these Terms and Conditions upon Legal Notice if:

- a) The other Party makes an assignment for the benefit of creditors, or admits in writing its inability to pay its debts as they mature;
- b) A trustee or receiver of any substantial part of the other Party's assets is appointed by any court; or
- c) A proceeding is instituted under any provision of the Federal Bankruptcy Laws by or against the other Party, and such proceeding is acquiesced in or is not dismissed within 60 days or results in an adjudication in bankruptcy.

Notwithstanding the above, Customer's right to terminate pursuant to this section may only be invoked if CyberReef is unable to provide Customer with Managed Service under these Terms and Conditions because of the foregoing. If Customer terminates the Service pursuant to this section, it shall not be relieved of its obligation to pay for any Managed Service used. At any time during the term of these Terms and Conditions, CyberReef may require Customer to provide a deposit to secure payment based upon Customer's creditworthiness or payment history with CyberReef. Any such deposit shall not relieve Customer of its obligation to pay any CyberReef bills. CyberReef shall pay any interest required by law on such deposit.

8. Limitation of Liability:

CyberReef and its affiliates and contractors will have no liability to customer or any end user:

- a) If changes in the wireless service or in the CyberReef network, system, operations, equipment, policies or procedures render obsolete or outdated any equipment, hardware, devices or software provided by the customers to end users in conjunction with their use of the customer product or service; CyberReef will supply customer 60 days' notice of any such situation once notified by Verizon.

b) For any causes of action, losses or damages of any kind whatsoever arising out of

(I) Failures or defects in the CyberReef network or systems,

(II) Use of the customers product or service or customer's equipment, or

(III) Disabling of equipment pursuant to section 5.

c) For any injury to persons or property, losses (including any loss of business), damages, claims or demands of any kind or nature, including, but not limited to, use or inability to use the Managed Service or wireless service, equipment, reliance by any end user or customer on any data provided or obtained through use of the wireless service or equipment, any interruption, defect, error, virus, or delay in operation or transmission, any failure to transmit or any loss of data arising out of or in connection with these terms and conditions.

In no event shall CyberReef or its vendors be liable for losses, damages, claims or expenses of any kind arising out of the use or attempted use of, or inability to access, life support or monitoring systems or devices, 911 or E911, or other emergency number or services.

9. Limitation of Damages:

In no event shall CyberReef, its affiliates and contractors be liable to customer, any end user, or any of their respective employees or agents, or any third party, for any indirect, incidental, special, consequential or punitive damages.

10. Indemnification:

10.1. Mutual Indemnification: Each Party shall defend, indemnify, and hold harmless the other Party from any and all losses and damages claimed by a third party in any action or proceeding, against the indemnified Party alleging bodily injury (including death) or damage to property, caused by or alleged to have been caused by the negligence or other wrongful acts or omissions of the indemnifying Party, its employees and authorized agents while on the other Party's premises, including any final monetary judgments, settlements, reasonable costs and reasonable attorneys' fees awarded therein.

10.2. Customer Indemnity: CyberReef shall not be liable for, and Customer shall defend, indemnify, hold harmless, and forever discharge CyberReef from all damages (including personal injury or death and damage to property), claims, actions, losses, liabilities, and other expenses (including reasonable attorneys' fees), regardless of the time when they occur, that arise out of any action brought by an End User or other third party in connection with:

a) Its or Customer's use of Managed Service or the Customer Product or Service (used independently or in conjunction with the Managed Service) or any Equipment or software used in conjunction therewith,

b) Communications with End Users

11. Notice and Defense:

The Party seeking indemnification shall:

- a) Provide the other Party with prompt Legal Notice of the claim;
- b) Allow the indemnifying Party to control the defense and settlement of the claim, provided, however, that the indemnifying Party shall not agree to any injunctive relief or settlement that obligates the indemnified Party to perform any obligation, make an admission of guilt, fault or culpability, or incur any expense, without such indemnified Party's prior written consent, which shall not be unreasonably withheld, delayed or conditioned;
- c) Have the right to obtain its own counsel at its own expense; and
- d) Provide reasonable cooperation to the indemnifying Party.

12. Violation of Authorized Use:

If CyberReef determines that Managed Service has been used in a manner not permitted by the Authorized Use policy in section 1.1, and Customer fails to cure such violation within thirty (30) days following Legal Notice from CyberReef informing Customer of such violation, then, in addition to such other rights as CyberReef may have under these Terms and Conditions or at law or in equity, CyberReef shall have the following rights:

- a) To suspend or terminate such Managed Service on notice to Customer;
- b) To retroactively bill Customer charges for such Managed Service at CyberReef's standard non-discounted rates applicable to services used in the manner such Managed Services were used by Customer. Such charges shall be paid by Customer within thirty (30) days of the date of CyberReef's bill.
- c) If Customer continues using Managed Services other than for the Authorized Use, CyberReef may deny such usage by Customer.

13. Dispute Resolution and Mandatory Arbitration:

Should a dispute arise under these Terms and Conditions; the Parties shall meet within 30 days after Legal Notice of such dispute is given to attempt to resolve the matter in good faith. Thereafter, the Parties agree to arbitrate any dispute arising out of these Terms and Conditions. Such arbitration shall be held before an independent arbitrator pursuant to the Wireless Industry Arbitration ("WIA") rules in effect at the time of the dispute, as modified by these Terms and Conditions and administered by the American Arbitration Association ("AAA"). The United States Arbitration Act, 9 USC §§1-16, as amended, shall govern the arbitration. In the event of any conflict, the WIA rules shall govern. No arbitration between the Parties may proceed on a class basis or be consolidated with any other arbitration without the written consent of all Parties. If the prohibition on class arbitrations set forth above is deemed unenforceable, then neither Party shall be required to arbitrate. Any award shall be accompanied by a written opinion of the arbitrator giving the reasons for the award and shall be binding upon the Parties with no right of appeal. If for any reason the provisions of these Terms and Conditions requiring arbitration are declared unenforceable, void, or voidable, or if any action or judicial proceeding is permitted, each Party waives any right it may have to trial by jury. Notwithstanding the above, either Party may seek preliminary and final injunctive relief in the event of the unauthorized disclosure of such Party's Confidential Information or intellectual property infringement.

14. Compliance with Laws:

14.1. Customer shall comply with all federal, state and local laws, treaties, rules, regulations and ordinances applicable to the Customer Product or Service, including

- a) All Federal Communications Commission rules and regulations,
- b) All privacy and security requirements, including those, if applicable, pertaining to medical devices or location-based services, and
- c) All consumer protection rules and regulations. Without limiting the scope of the foregoing, Customer agrees as follows:
 - I) It shall comply with Department of Treasury's Office of Foreign Assets Control (OFAC) regulations to not provide the Managed Service to any individual or entity appearing on the OFAC Specially Designated Nationals (SDN) list or that is the subject of an embargo or sanction;
 - II) All functionality provided by Customer does and will comply in all respects with the Communications Assistance for Law Enforcement Act ("CALEA"). Customer shall certify in writing on each anniversary of the Effective Date or on CyberReef's reasonable request, that it is in compliance with its obligations under this Section;
 - III) Customer shall comply with any federal, state and local laws, rules, regulations or legal requirements.

14.2. If Customer elects to receive government funds,

- I) Customer shall comply in all respects with any and all federal and state laws, rules, regulations and orders that apply to carriers receiving such funds, including, but not limited to, any exempting any certain class of End Users from assessment of any tax, fee, duty, surcharge or other tax-like charge (including, but not limited to, any restriction on the assessment of universal service fund surcharges or number portability fees against qualified, low-income subscribers),
- II) CyberReef shall have no obligation to Customer to make modifications or changes to any of its processes or procedures, the Managed Service or the CyberReef network used by Customer, in satisfaction of any federal or state requirements related to receipt of government funds, and
- III) CyberReef shall have no obligation to Customer to furnish, maintain or retain information in satisfaction of any federal or state requirements related to Customer's receipt of government funds in the form of reports, records, maps, certifications, documentation or other forms of data.

15. Confidential Information:

15.1. Use and Disclosure: Each Party shall hold in confidence Confidential Information received from the other Party from the Commencement Date and a period of 2 years thereafter. "Confidential

Information” means information (in written, graphic, oral or other tangible or intangible form) concerning the disclosing party’s business, customers, products, services, trade secrets and personnel, and designated as confidential by the disclosing party (if tangible information) by conspicuous markings or (if oral information) by announcement at the time of initial disclosure and written documentation thereof within 30 days thereafter, or if not so marked or announced and documented should reasonably have been understood as being confidential information of the disclosing party either because of other legends or markings, the circumstances of disclosure or the nature of the information itself.

Confidential Information may include proprietary material as well as material subject to and protected by laws regarding secrecy of communications or trade secrets and may include information acquired by the disclosing party from a third party under an obligation of confidentiality. Confidential Information also shall include the pricing and other terms and conditions of these Terms and Conditions, which both Parties shall be required to hold in confidence. Neither Party shall disclose Confidential Information of the other Party to any third party or use Confidential Information of the other Party for any purpose other than as specified in these Terms and Conditions. The Parties may disclose Confidential Information of the other Party to their agents that have a need to know under these Terms and Conditions and are bound by non-disclosure obligations that are substantially similar to those set forth herein. Customer’s agents are subject to the additional requirements set forth in the “Customer’s Use of Third Parties” section below. Notwithstanding anything to the contrary set forth herein, Customer must obtain CyberReef’s written permission prior to disclosing any Confidential Information of CyberReef to any direct competitor of CyberReef .

15.2. General Exclusions: The foregoing restrictions shall not apply to information to the extent that it:

- a) Is or becomes publicly available through no act or omission of the receiving Party;
- b) Was already in the lawful possession of the receiving Party without an obligation of confidentiality;
- c) Is lawfully disclosed to the receiving Party by a third party without restriction;
- d) Is required to be disclosed by subpoena or other legal process, limited to the extent required by the terms of such subpoena or other legal process;
- e) Is approved in writing by the disclosing Party for further disclosure;
- f) Is independently developed without reference to the Confidential Information and is so documented by the receiving Party; or
- g) Is required to port telephone numbers.
- h) Is required by local state legislature such as the Public Records Act in each state.

CyberReef shall not be deemed to have received Confidential Information of Customer solely because Customer receives, transmits, obtains or otherwise exchanges such information through the use of the Managed Service, or any other CyberReef service to Customer involving the hosting, transport or other similar handling of such information.

15.3. Permitted Usage and Disclosure of Confidential Information: Nothing contained herein shall prevent either Party from using or disclosing Confidential Information for the purposes of disclosing

general information about these Terms and Conditions in limited internal announcements to its employees.

16. Marks:

16.1. Customer hereby acknowledges that the CyberReef owned and/or licensed name(s), trademarks, and service marks ("CyberReef Marks") are the sole property of CyberReef and/or its parents or affiliates, and are good, valid, and enforceable in law and equity. Customer shall not challenge or assist in challenging the validity of registrations thereof, or engage in any activities or commit any acts, directly or indirectly, which may contest, dispute or otherwise impair the right, title and interest of CyberReef or its parents or affiliates therein. Customer neither has nor shall acquire, any right, title or interest in or to the CyberReef Marks.

16.2. Customer shall not use any of the CyberReef Marks, or any language from which the CyberReef Marks may be inferred or implied, for any reason unless CyberReef has expressly approved such usage in writing in advance. Any unauthorized direct or implied use of the CyberReef Marks by Customer shall be a material breach of these Terms and Conditions and shall constitute an infringement of the CyberReef Marks.

17. Customer's Use of Third Parties:

Customer may employ third parties to make purchases, act as an Authorized Contact or perform other telecommunications management services under these Terms and Conditions, subject to the following:

- a) Customer must notify CyberReef in writing prior to use of a third party and identify the scope of such third party's authority;
- b) Customer grants CyberReef permission to disclose to such third party any information relating to the Terms and Conditions or Customer's account(s);
- c) Such third party must be bound by confidentiality obligations that are substantially similar to those in these Terms and Conditions;
- d) CyberReef reserves the right to require such third party to enter into a non-disclosure agreement with CyberReef; and
- e) Customer's right to terminate the Service shall remain solely with Customer.

18. No Agency:

The Parties are independent contractors. Customer is not authorized to act as an agent for or legal representative of CyberReef and does not have and shall not represent that it has any authority to assume or create any obligation on behalf of CyberReef.

19. Assignment:

Provided an assignee possesses the financial and operational capabilities to perform under these Terms and Conditions and agrees in writing to assume and fully discharge all of the duties and obligations of the assignor arising under these Terms and Conditions, either Party may assign these Terms and Conditions in its entirety, without the other Party's consent, to either of the following:

- a) Any entity that controls, is controlled by or is under common control with the assigning Party;
- b) A successor in interest to all or substantially all of the assets and business of the assigning Party.

Customer may not assign its rights or delegate its duties under these Terms and Conditions to any direct competitor of CyberReef without the prior written consent of CyberReef. Except for the foregoing, neither Party may assign its rights under these Terms and Conditions to any other entity without the prior written consent of the other Party, which shall not be unreasonably withheld, delayed or conditioned. Subject to the provisions of this section, these Terms and Conditions shall inure to the benefit of and be binding upon the respective successors and assigns, if any, of the Parties hereto.

20. Termination:

Except as otherwise expressly stated in these Terms and Conditions, either Party shall have the right to terminate the Service for default if

- a) The defaulting Party fails to comply with any material term, condition, or obligation of these Terms and Conditions;
- b) The non-defaulting Party provides Legal Notice to the defaulting Party specifying the default; and
- c) The defaulting Party fails to cure such default within thirty (30) days after receipt of such notice. If the defaulting Party has commenced to cure the default but it cannot reasonably be cured within the thirty (30) day period, then the non-defaulting Party may not terminate the Service as long as the defaulting Party takes appropriate steps to cure the default at the earliest reasonable time.

21. Force Majeure:

Any failure of CyberReef or Customer to perform hereunder shall be excused if caused by failure of a third-party wireless or telecommunications provider serving a particular area, power failure, national emergency, interference by any governmental agency, acts of God, strikes, other labor disturbance, severe weather conditions, fire, terrorism, riots, war, earthquakes, or any other causes beyond CyberReef' or Customer's reasonable control.

22. Notices:

Whenever these Terms and Conditions calls for a "Legal Notice" to be given, notice shall be given in writing and shall be valid and sufficient if dispatched by:

- a) Registered or certified mail, postage prepaid,
- b) Hand delivery or

c) A nationally recognized express courier. Notice to Customer may be made to Customer's designated Authorized Contact(s). Any notice given in accordance with the foregoing requirements shall be deemed effective upon delivery. All other notices and communications related to these Terms and Conditions may be made via mail or e-mail to an Authorized Contact, mail to the billing address on the account, and/or message with Customer's monthly bill.

d) addressed to the signer of this document or his designated replacement if no longer with the company.

23. Governing Law, Venue and Jurisdiction:

Subject to the provisions of the "Dispute Resolution and Mandatory Arbitration" section above, the validity, construction and performance of these Terms and Conditions shall be governed and interpreted in accordance with the laws of the State of Louisiana, without reference to its conflict of laws or other rules that would require the application of the laws of another jurisdiction. Each Party submits to personal jurisdiction exclusively in Louisiana and waives all objections to a Louisiana venue.

24. Counterparts and Admissibility of Copies:

These Terms and Conditions may be executed in counterparts each of which when executed and delivered shall be deemed to be an original and all of which together shall constitute one and the same instrument. An electronic or facsimile copy of the executed Terms and Conditions or counterpart shall be deemed and shall have the same legal force and effect as, an original document.

25. No Waiver:

Any forbearance or delay on the part of either Party in enforcing any rights under these Terms and Conditions shall not be construed as a waiver of such rights. Any grant of a waiver in one instance shall not be construed as a continuing waiver in all similar instances. No provision of these Terms and Conditions shall be considered waived unless expressly waived in writing, signed by the party against whom enforcement of such provision is sought.

26. Severability:

If any provision of these Terms and Conditions is held to be invalid, illegal or unenforceable by a court of competent jurisdiction, the remaining provisions of these Terms and Conditions shall remain in full force and effect. Moreover, the Parties agree that the invalid, illegal or unenforceable provision shall be enforced to the maximum extent permitted by law in accordance with the intention of the Parties as expressed by such provision.

27. CyberReef Support Policy:

See attachment A.

28. M2M Service Plan:

See attachment B.

29. CyberReef UptimePlus:

See attachment C for additional Terms & Conditions specific only to UptimePlus Service.

30. Survival:

Termination of the Service shall not affect either Party's accrued rights or obligations under these Terms and Conditions as they exist at the time of termination, or any rights or obligations that either expressly or by implication continue after the Service has ended.

31. Terms and Conditions, including all attachments:

These Terms and Conditions including any attachments and the terms and conditions of any Managed Services, options, features, and applications (collectively, "Service Offerings") selected by Customer, constitute the entire agreement between the Parties with respect to the subject matter hereof. These terms and conditions shall prevail over any conflicting terms and conditions of a Service Offering, except for terms and conditions that are specific to the use of the selected service. These Terms and Conditions shall not be amended or modified without specific written agreement signed by both Parties. In no event shall any terms and conditions be added or modified by purchase order.

The Customer or Customer's duly authorized representative(s) agrees to these Terms & Conditions as of the date set forth below:

Company Name: _____

Authorized Representative

Name: _____

Title: _____

Signature: _____

Date: _____

ATTACHMENT A:

CyberReef Support Policy

Hours of Operation

Central Standard Time applies. CyberReef normal support hours are 7AM to 8 PM Central Time Zone. For any planned shutdown of any private network resource, CyberReef customers will be notified via e-mail at least 24 hours in advance.

Reporting Procedure

For failures with any of CyberReef services during non-business hours, the automated operator should be contacted at **251-279-0749** and leave a voicemail. The voicemail will be forwarded to the CyberReef Tech team.

Please see below our definitions of Call-in Classifications.

Critical – Network/Server or critical use Modem – response in an hour or less

Major – A device connection issue with non-critical equipment 12-24 hours

Minor – Data usage report or general information questions – 24 hours

For non-critical reported problems, (**Major** or **Minor**) the tech team will handle the next business day of after hours.

After Hours Support Policy

CyberReef is committed to making available critical private network and bandwidth management server resources to our customers 24/7. Our team will provide on-call support coverage in the event of unexpected failure or significant problems with **critical** resources during non-business hours. For a **critical** issue, support will be available 24/7.

Resolution of any problem during non-business hours may be dependent upon the nature of the problem and the availability of resources or service and parts from third party vendors. CyberReef will assess a reported problem and determine a reasonable resolution plan based upon the severity of the problem and resources required. CyberReef will work to resolve the problem as quickly as possible. For a problem that requires more than four hours to resolve, a status message will be forwarded to our private network customer's point of contact.

ATTACHMENT B:

M2M Service Plan

Megabyte (MB) Data Plans: M2M data usage is rounded to next full kilobyte at end of each billing cycle. Any unused portion of the megabyte allowance is lost. Equipment will not indicate kilobyte usage.

International Access Data Roaming: In the Canadian Broadband and Canadian Enhanced Services Rate and Coverage Areas, usage will be charged at a rate of \$0.004/KB or \$4.10/MB. In the Mexican Enhanced Services Rate and Coverage Area, usage will be charged at a rate of \$0.01/KB or \$10.24/MB. In the Bermuda, China, Dominican Republic, Guam, India, Israel, Saipan and South Korea Enhanced Services Rate and Coverage Areas, usage will be billed at a rate of \$0.04/KB or \$40.96/MB.

A data session is inactive when no data is being transferred and may seem inactive while data is actively being transferred to a device or seem active when actually cached and not transferring data. Customer must maintain virus protection when accessing the service and is responsible for all data sent and received including "overhead" (data that is in addition to user-transmitted data, including control, operational and routing instructions, error-checking characters as well as retransmissions of user-data messages that are received in error) whether such data is actually received. CyberReef will not be liable for problems receiving Service that result from Customer's device.

ATTACHMENT C:

Terms & Conditions ONLY applicable to “UptimePlus” Service

UptimePlus: Unlimited Rate Plan

1. UptimePlus (UT+) unlimited is a backup service and is not intended to provide primary connectivity.
2. UT+ is an unlimited backup service for organizations of all sizes including SMBs, multi-location, large enterprises, etc.
3. UT+ utilizes web filtering and *blocks access to the following website categories:
 - a. Abortion
 - b. Abused Drugs
 - c. Adult
 - d. Alcohol and Tobacco
 - e. Command and Control
 - f. Copyright Infringement
 - g. Dating
 - h. Dynamic DNS
 - i. Extremism
 - j. Gambling
 - k. Games
 - l. Hacking
 - m. Insufficient Content
 - n. Malware
 - o. Music
 - p. Nudity
 - q. Parked
 - r. Peer-to-Peer
 - s. Personal Sites and Blogs
 - t. Philosophy and Political Advocacy
 - u. Phishing
 - v. Proxy Avoidance and Anonymizers
 - w. Questionable
 - x. Recreation and Hobbies
 - y. Sex Education
 - z. Shareware and Freeware
 - aa. Social Networking
 - bb. Sports
 - cc. Streaming Media
 - dd. Swimsuits and Intimate Apparel
 - ee. Weapons
 - ff. Web Advertisements
4. UT+ provide alerts of failover to designated customer contact(s) and CyberReef expects primary connectivity to be restored within 24 hours.
5. If primary connectivity is not restored within 24 hours, at its discretion, CyberReef may bill customer \$10/GB for data consumption over 10GB.

6. *Allowed Categories
- a. Auctions
 - b. Business and Economy
 - c. Computer and Internet Info
 - d. Content Delivery Networks
 - e. Educational Institutions
 - f. Entertainment and Arts
 - g. Financial Services
 - h. Government
 - i. Health and Medicine
 - j. Home and Garden
 - k. Hunting and Fishing
 - l. Internet Communications and Telephony
 - m. Internet Portals
 - n. Job Search
 - o. Legal
 - p. Motor Vehicles
 - q. News
 - r. Not Resolved
 - s. Online Storage and Backup
 - t. Private IP Addresses
 - u. Real Estate
 - v. Reference and Research
 - w. Religion
 - x. Search Engines
 - y. Shopping
 - z. Society
 - aa. Stock Advice and Tools
 - bb. Training and Tools
 - cc. Translation
 - dd. Travel
 - ee. Unknown
 - ff. Web-based Email
 - gg. Web Hosting

**CyberReef reserves the right to change UT+ web filtering at its discretion without prior customer notification.*

- 7. Each SIM for UptimePlus service requires a one-time \$25 activation fee.
- 8. Each SIM plus Hardware for UptimePlus service requires a one-time \$50 activation & set-up fee.
- 9. If Hardware is provided the plan requires a 3-year term commitment with \$250 early termination fee.

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh
Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)
Subcategory N: Secure LAN Access

Client Company name:	WEC Energy Group
Client name of contact:	Steve Liegl
Client contact title:	Director Infrastructure and Operations
Client is a daily user, occasional user, etc.:	Daily User

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to James Rose no later than Friday, November 6th.

Thank you for your assistance in this process.

- 1. For what services do you use USCC's product, and how long have you been USCC's customer?**
We currently use USCC for voice and data services across our field crew members. These crew members provide support to our electric and gas distribution system. Customer since 1988.

- 2. Would you recommend USCC to other customers? Why?**
Yes, the attention that our account team has on the account and their ability to provide services directly related to our needs saves a lot of time. In addition, coverage and network quality has been key attributes supporting our desire to put our wireless voice and data needs on the USCC network.

- 3. Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

USCC has provided timely response to the effort needed to establish a private VPN within our environment. This created an easy to use solution for our end users.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

We have not had to file any complaints, nor have we had any major disruptions impacting our business in recent years.

- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

All voice and data products continue to meet our business needs through their reliability and expansive wireless service. The expansion of service in Wisconsin has been a great benefit to our mobile users as well.

- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

Nothing at this time.

- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

Nothing at this time

- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

All products have been described. We have business with competing wireless carriers, and I would say that our needs are met with the USCC account team and network capabilities.

Appendix S

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

**Subcategories J and O: IoT Management and Utility
Operations, Monitoring and Support**

LEC iQ2



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
iQ2-Remote Monitoring and Control Industrial IoT Platform.
- b. General Application Area
Subcategories J and O: IoT Management, Utility Operations, Monitoring and Support
- c. General capabilities provided
Remote monitor and control of industrial and municipal assets. Including, but not limited to: Pumps, compressors, generators, water/wastewater infrastructure, utility/energy infrastructure, remote sensors, ITS assets, etc.
- d. Expected impact on cost/performance/functionality, etc.
 - Reduced truck-rolls to remote sites and infrastructure - reduces costs and increases safety
 - Establish state and federal compliance for remote monitoring of disconnected or unmanaged field assets
 - Provide real-time and historical data analytics to improve operational efficiency and reduce related costs
 - Provide alerting and alarming to mission critical assets to reduce risk of system failures and costs associated with such failures
 - The cloud-based application provides real-time insight into asset performance via any web-enabled device or handset decreasing response time to critical field failures.
 - Highly flexible system allows low-cost and simple integration with existing systems.
 - Non-proprietary hardware allows for quick availability and competitive costs on off-the shelf hardware across multiple OEM's.
- e. Subcontractors/partners involved in delivering service
UScellular partners with LEC to provide this solution.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
 - Highly flexible application that easily integrates with existing field assets such as PLC's HMI's and RTU's.
 - Simple configuration process for digital, analog, ethernet and RS485 data types and protocols
 - Remote access capabilities to PLC's and existing infrastructure through the cellular or non-cellular edge gateway
 - User interface fully functional for remote monitoring and control via any web-enabled device.

- No coding or software development in order to integrate most edge assets
 - Speed and simplicity of deployment reduces deployment costs and reduces need for highly technical staffing resources
 - Ongoing support and maintenance do not require professional engineering resources
 - Alerting and alarming functions reduce field failures and provide insight into root cause and needed field support
 - Daily, Weekly and Monthly reporting provide data needed for compliance and granular analytics
- b. Applicability to government needs
This remote monitor and control technology supports a broad application and many different use cases.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
Several hundred sites throughout the US and Canada. References readily available based on application.
- IIoT water/wastewater market*
Ronnie Jones
Aqua Products, Inc
Sarasota, FL 32505
850-469-1133
- d. Overall interoperability of turnkey system for government use
API's can be made available to integrate with other systems in use.
- e. Accessories available for turnkey offering
- Cellular communication gateways
 - UL 508A Certified IoT-Ready Panels-Gateway, I/O, Power Supply, UPS backup, antenna, wiring, in all in a ready-to-deploy enclosure
 - Cellular antennas and cable
 - HMI's, PLC's and other automation hardware
 - Professional Services-Engineering and Integration
- f. Thoroughness of the vetting process used to select partners
We do not use partners for this application. Should installs be required as part of a turnkey solution, third-party recommendations can be provided.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
Full Factory Acceptance Test (FAT) completed and documented prior to shipment/deployment.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination

Site Survey and Solution Discovery planning is completed by the assigned Project Manager through collaboration with client. Site Survey Document is completed and fully documented based on project needs. Site Survey is provided to customer for final acceptance and approval. Automation requirements are developed and reviewed with client and formal customer sign-off completed upon acceptance of any control narrative.

b. Project coordination

LEC Project Management and Engineering Resources are assigned based on application/solution type and needs. Project management stays engaged throughout every stage of the process. Depending on project scope, reoccurring team calls are scheduled to meet project demands, timelines and expectations with Project Reports provided on a consistent basis.

c. Installation and Testing process

Pilots are a common process in order to optimize the solution requirements and deployment model. Pre-Install testing is completed through FAT testing at LEC facilities prior to shipment, installation, and deployment. Installation is typically customer driven due to simplicity of install or utilizing existing 3rd party municipal vendor. All installation instructions and wiring diagrams are provided with real-time support during field installation and final functional testing.

d. Client Infrastructure and support assessment process

LEC provides infrastructure and assessment through the site-survey and then finalized during the completion of the quality assessment process.

e. End user Acceptance process

- Completion of LEC iQ2 Quality Assurance Process Document
- 30, 60, and 90 Day QA customer engagement process
- Solution Training/Refinement process
- SolveIT Support Tool training
- Final customer sign-off at 90 days

f. Approach to maintenance and support

- 24/7/365 Access to SolveIT support ticketing system is standard
- Advanced notices of system maintenance and upgrades provided
- iQ2 Feature and Functionality upgrade notices provided
- Standard Support Services as provided in iQ2 Services Agreement
- Extended Support Services available

g. Initial and Ongoing Training provided

- iQ2 User and Admin Training prior to deployment
- 30, 60, and 90-day Training Program as part of the iQ2 Quality Assurance process
- Training for iQ2 feature additions provided upon request
- End user and Admin Video Training series available to all LEC Customers

h. On-going support and enhancement over the life of the agreement

See Attached LEC iQ2 Services Agreement

4 - Service Factors:

a. Description of related services included in Turnkey Solution

LEC Turnkey Solutions include:

- Customer Site Survey Support
- IIoT Communications Hardware-From list of iQ2-Ready UL 508A Certified devices
- Delivery of all related wiring and installation diagrams
- Installation support
- Private Cellular Network Connectivity
- Site Engineering Support Admin and User Access to the iQ2 Remote Monitoring and Control Platform
- 24/7/364 Access to SolveIT Support Tool

b. Experience and qualifications of partners and subcontractors

LEC does not utilize partners or subcontractors on a standard deployment.

c. Description of Additional Integration and Consulting Services provided

- Site Survey Support Services
- IIoT Engineering Support Services
- Network Engineering Services
- LEC Installation Services

We have a full Products and Services guide that is available upon request.

EXHIBIT D

SUPPLIER TERMS AND CONDITIONS

iQPulse™ TERMS AND CONDITIONS AGREEMENT

YOU MUST READ THIS iQPulse™ TERMS AND CONDITIONS AGREEMENT CAREFULLY. THE SERVICE IS PROVIDED TO THE CUSTOMER SUBJECT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT.

Section 1. Definitions.

1.1 "Agreement" means this iQPulse™ Terms and Conditions Agreement, as may be amended from time to time in accordance with the terms and conditions hereof.

1.2 "Communication Facility(ies)" means any wired or wireless instrumentality or service (or any combination thereof) used as a pathway for enabling Customer's use of the Service, including the Internet.

1.3 "Company" means LEC, Inc., a Mississippi business corporation, having its principal offices located at 110 Excell Drive Pearl, Mississippi 39208, together with each entity that it directly or indirectly owns or controls.

1.4 "Components" means the individual modules, features or products that make up the System. From time to time, new Components may be introduced, and access to those Components may be restricted depending on the terms of the particular Service.

1.5 "Connectivity Agreement" means the agreement between USCC and Customer governing Customer's subscription to any Communication Facility(ies) provided by USCC in connection with the Service.

1.6 "Customer" means the individual or entity who is a subscriber to any Communication Facility(ies) provided by USCC in connection with the Service.

1.7 "Customer Data" means any of Customer's information, documents, or electronic files that are either (A) transmitted through an Endpoint in connection with the Service, or (B) provided to Company hereunder for any purpose. At all times Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, security, appropriateness, ownership and permanent storage and safekeeping of all Customer Data.

1.8 "Effective Date" means the date of Customer's acceptance of this Agreement.

1.9 "Emergency System Maintenance" means any extraordinary, unscheduled maintenance to the System (or its Components) performed by Company for the purpose of immediately addressing any issue that affects the security or availability of the System.

1.10 "Endpoint(s)" means any iQPulse™ enabled device, or other device or asset generating Customer Data that is populated into the System.

1.11 "Event(s) of Default" means Customer's failure to perform or observe any other term, condition, or covenant to be performed by it under this Agreement.

1.12 "Force Majeure Event" means any (A) act(s) of war, hostility, or sabotage, including denial of service attacks; (B) act(s) of God; (C) electrical, Internet telecommunication outage or security breach that is not caused by the obligated Party; (D) government restrictions (including the denial or cancellation of any export or other license); and/or (E) any other event outside the reasonable control of the obligated Party.

1.13 "Notice" means any notice(s), consent(s), communication(s) and exchanges of information between the Parties as may be required hereunder. All Notices shall be provided in writing and shall be delivered personally, by registered or certified letter (return receipt requested), by courier or facsimile, and unless otherwise provided for in this Agreement shall be deemed effectively served (A) if by personal delivery, immediately upon such delivery; (B) if by registered or certified mail, five (5) calendar days after mailing; (C) if by courier, three (3) days after deposit; and (D) if by facsimile, immediately upon dispatch if receipt is confirmed electronically. All Notices shall be sent to the appropriate receiving Party's addresses as follows (or such other address as may have been furnished by or on behalf of such Party by like Notice): (i) if to Company – LEC, Inc., Post Office Box 127, Brandon, Mississippi 39043-0127; and (ii) if to Customer – the address identified as Customer's address in the Connectivity Agreement.

1.14 "Party" means Company or Customer, and every reference to a Party includes its successors and permitted assigns; and "Parties" means, collectively, Company and Customer and their respective successors and permitted assigns.

1.15 "Regular System Maintenance" means any regular, scheduled maintenance to the System (or its Components) performed by Company for the purpose of improving the functionality or security of the System.

1.16 "Service" means access to the System and its Components, together with certain additional related services, which depending upon the particular Service used by Customer may or may not include (A) temporary storage or backup of Customer Data; (B) hosting of Customer remote-site web pages(s); (C) remote troubleshooting (to the extent it relates to an embedded System device client application); (D) user-access management; (E) Customer support services; and (F) any other related services that Company may make available from time to time. Expressly excluded from the definition of Service are any and all Communication Facilities provided by Customer and/or any Third Party with whom Customer has an agreement to provide Communication Facilities.

1.17 "System" means the iQPulse™ platform, including any updates and improvements relating thereto and any derivative works of the foregoing. The System is made up of individual Components.

1.18 "Third Party" means any person or entity that is not a Party to this Agreement.

1.19 "USCC" means USCC Services, LLC, a Delaware limited liability company, having its principal offices located at 8410 W. Bryn Mawr, Chicago, Illinois 60631, together with each entity that its parent company United States Cellular Corporation directly or indirectly owns or controls. USCC is acting as a reseller of the Service.

Section 2. Rights and Restrictions of Use of the Service.

2.1 Customer Use Rights. During the Term hereof (as hereinafter defined) and subject to the terms and conditions of this Agreement, Company hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable right to connect the Endpoints to the Service for Customer's business purposes. The use right in the preceding sentence is strictly limited to the number of Endpoints as identified in the Connectivity Agreement. Said use rights are non-transferable, except in the event of a voluntary transfer of substantially all assets by Customer to a transferee which executes Company's form of agreement agreeing to be bound by all of the terms and conditions of this Agreement. All rights in and to the use of the Service not expressly granted to Customer herein are reserved to Company, and Customer agrees that Customer does not acquire any rights to use the Service in excess of the scope and/or duration of the term of this Agreement; provided, however, that Customer shall retain all ownership and intellectual property rights in and to the Customer Data. The rights of Customer to use the Service on a particular Endpoint cannot be shared or used by, on or for more than one Endpoint. To the extent that it may be appropriate or necessary in any particular Customer application to utilize any Third Party hardware,

software or technology with the Service, Customer's right to use such Third Party hardware, software or technology shall be governed by the terms of the applicable Third Party hardware, software or technology license agreement and not under this Agreement. To the extent that the Service may enable Customer to add links to web sites and access to content, products and services of any third parties (including users, advertisers, affiliates and sponsors of such third parties), Company is not responsible for any such Third Party web sites or Third Party content provided on or through the Service and Customer assumes and shall bear any and all risks associated with the access and use of such web sites and Third Party content, products and services. Upon the expiration or earlier termination of this Agreement as provided herein, all rights of Customer to use the Service shall terminate.

2.2 Availability of Service. At all times during the Term hereof, Company warrants that Company will provide to Customer access to the Service on a twenty-four (24) hours, seven (7) days per week basis at an availability rate of at least ninety-nine point nine percent (99.9%) (the "Service Uptime"). Service Uptime shall be calculated to the nearest minute occurring during each calendar month of the Term and shall be continuously monitored through Company's automated systems.

2.3 System Maintenance. Company may perform Regular System Maintenance on an as-needed basis (typically occurring between the hours of 9:00 P.M. and 4:00 A.M. Pacific Time), which in certain circumstances may result in an interruption of Service Uptime. Company will provide to Customer a minimum of fifteen (15) days advance Notice of any Regular System Maintenance to be conducted, and in circumstances where an interruption in Service Uptime is expected to occur shall specify in said Notice the anticipated duration of such interruption. In unexpected circumstances where Company is required to perform Emergency System Maintenance, Company will provide to Customer advance Notice of any Emergency System Maintenance as reasonably possible under the circumstances.

2.4 Storage and Backup of Customer Data. In the event that the Service subscribed to by Customer includes the temporary storage or backup of Customer Data (as applicable), Company will temporarily store or backup any Customer Data populated to the System (or portion thereof as may be designated by Customer) up to a maximum of either (A) a period of twelve (12) months, or (B) a limit of five hundred thousand (500,000) database records, whichever occurs first; provided, however, that the foregoing database record limit may be affected by the configuration of the device(s) comprising each Endpoint and/or the specific data value update rates determined by Customer's use of the Service.

2.5 Customer Support. Company agrees to provide normal Customer support on weekdays between the hours of 8:00 A.M. and 5:00 P.M. Central Time, during which time Company will respond to a request for Customer support within one (1) hour or less. Further, Company agrees to provide after-hours Customer support on weekdays between the hours of 5:00 P.M. and 8:00 A.M. Central Time and on weekends via Company's solveIT@ ticketing system, during which time Company will respond to a request for Customer support no later than 10:00 A.M. Eastern Time the following business day.

2.6 Company Use Rights. During the Term and subject to the terms and conditions of this Agreement, Customer hereby grants to Company a non-exclusive, non-transferable, non-sublicensable right to use, copy, transmit, store, modify and display the Customer Data solely for purposes of Customer's use of the Service; otherwise, Company shall not use the Customer Data except to improve the Service and/or as necessary to perform its obligations hereunder. Company may compile statistical information related to the performance of the Service, and at its election make such information publicly available, provided that such information does not incorporate Customer's identify, any Customer Data, and/or any of Customer's Confidential Information (as hereinafter defined), and Company shall retain all intellectual property rights in and to such information.

2.7 Customer Use Restrictions. At all times during the Term hereof, Customer expressly covenants and agrees not to use or permit use of the Service, including without limitation by uploading, emailing, posting, publishing or otherwise transmitting any Customer Data or other material, for any purpose that may (A) menace or harass any person or cause damage or injury to any person or property; (B) involve

the publication of any material that is false, defamatory, harassing or obscene; (C) violate privacy rights or promote bigotry, racism, hatred or harm; (D) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (E) constitute an infringement of intellectual property or other proprietary rights of any Third Party; or (F) otherwise violate applicable laws, ordinances or regulations. In addition to any other rights afforded to Company hereunder, Company expressly reserves the right to suspend access to the Service for any violation of the foregoing restrictions and shall have no liability to Customer in the event that such action is taken. Customer expressly acknowledges that the Service is not intended for use with protected health information under HIPAA, credit card numbers, financial account numbers, or other similarly-sensitive personal information, and that Customer assumes all risk arising from use of any such sensitive information with the Service, including the risk of any inadvertent disclosure or unauthorized access thereto. Customer is responsible for ensuring that Customer's use of the Service is in compliance with all applicable laws and governmental regulations (including without limitation those set forth in Section 7 of this Agreement), and Customer acknowledges that Customer assumes all risk arising from any such use that is not compliant with applicable laws and regulations.

2.8 Other Restrictions. In addition to those restrictions set forth in Section 2 hereof, with respect to either the Service and/or the System, as applicable, Customer shall not, directly, indirectly, alone, or with another party either (A) remove or modify any Company markings or any statement or declaration of Company's proprietary rights; copy, disassemble, reverse engineer, or decompile the System; (B) modify, create derivative works based upon, or translate the System; (C) license, sell, rent, lease, transfer, grant any rights in or otherwise commercially exploit the Service in any form to any other party; (D) access or use the Service in order to build or support, and/or assist a Third Party in building or supporting, products or services competitive to Company; (E) other than the Customer Data, disclose the results of the Service without Company's prior written consent; or (F) attempt to do any of the foregoing or cause or permit any Third Party to do or attempt to do any of the foregoing. At all times Company shall own all right, title and interest in and to any and all intellectual property rights (including all derivatives or improvements thereof) in the Service, and any suggestions, enhancement requests, feedback, recommendations or other information provided by Customer relating to the Service.

3. Non-Disclosure of Confidential Information. By virtue of this Agreement, the Parties may have access to one-another's information that the owning Party considers confidential in nature (the "Confidential Information"). Accordingly, each Party expressly covenants and agrees to disclose only information that is required for the performance of their respective obligations under this Agreement. The term "Confidential Information" shall also include the terms under this Agreement, any Customer Data residing in the System environment, and all information clearly identified as confidential at the time of its disclosure. However, a Party's Confidential Information shall not include information that: (A) is or becomes a part of the public domain through no act or omission of the other Party; (B) was in the other Party's lawful possession prior to the disclosure and had not been obtained by the other Party either directly or indirectly from the disclosing Party; (C) is lawfully disclosed to the other Party by a Third Party without restriction on the disclosure; or (D) is independently developed by the other Party. Each Party agrees to hold one another's Confidential Information in confidence for a period of three (3) years subsequent to the expiration or termination of this Agreement, and further agrees to disclose Confidential Information only to its employees or agents who are required to protect it against unauthorized disclosure in a manner no less protective than under this Agreement, and in any event only for the purpose of performing a Party's obligations hereunder. Nothing shall prevent either Party from disclosing the terms under this Agreement in any legal proceeding arising from or in connection with this Agreement or from disclosing the Confidential Information to a governmental entity as may be required by applicable law.

Section 4. Term and Termination.

4.1 Term. The term of this Agreement (the "Term") commences on the Effective Date and remains in effect for the duration of the term of the Connectivity Agreement. The Term will automatically terminate upon the termination or expiration of the Connectivity Agreement. For a period of up to thirty (30)

days subsequent to the effective date of the expiration or termination of this Agreement, upon receipt of written request Company may permit Customer to access the Service solely to the extent necessary for Customer to retrieve any Customer Data to the extent that any such Customer Data resides in the System environment; provided, however, that Customer expressly acknowledges and agrees that Company has no obligation to retain any Customer Data and that any Customer Data residing in the System environment may be irretrievably deleted at any time after thirty (30) days subsequent to the expiration or termination of this Agreement.

4.2 Termination of Service. The Service may be terminated by Company upon the occurrence of an Event of Default by Customer if such Event of Default is not cured by Customer within thirty (30) days subsequent to receipt of a Notice of the Event of Default; provided, however, that in any case of any violation by Customer of Section 2 of this Agreement, the Service may be terminated immediately by the Company.

Section 5. Warranty Disclaimer and Liability.

5.1 Warranty Disclaimer. AS COMPANY DOES NOT CONTROL THE TRANSFER OF DATA OVER OR THROUGH ANY COMMUNICATION FACILITIES, CUSTOMER EXPRESSLY ACKNOWLEDGES AND AGREES THAT (A) COMPANY DOES NOT GUARANTEE THAT THE SERVICE WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT COMPANY WILL BE ABLE TO CORRECT ALL SERVICE ERRORS; (B) THE SERVICE MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATION FACILITIES; AND (C) COMPANY IS NOT RESPONSIBLE FOR ANY ERRORS, DELAYS, DELIVERY FAILURES, OR OTHER DAMAGES THAT MAY RESULTING FROM SUCH PROBLEMS. TO THE EXTENT NOT PROHIBITED BY LAW, EXCEPT AS OTHERWISE PROVIDED HEREIN THERE ARE NO EXPRESS OR IMPLIED WARRANTIES FOR OR CONDITIONS TO THE SERVICE HEREUNDER, INCLUDING COMPATIBILITY OF THE SERVICE WITH ANY SPECIFIC HARDWARE, SYSTEMS, COMMUNICATION FACILITIES, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

5.2 Liability Disclaimer. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF ANY CUSTOMER DATA, REVENUE OR PROFITS (EXCLUDING FEES PAYABLE BY CUSTOMER TO COMPANY UNDER THIS AGREEMENT). COMPANY'S MAXIMUM LIABILITY TO CUSTOMER FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNTS ACTUALLY PAID BY CUSTOMER TO USCC (AS RESELLER) FOR THE SERVICE THAT IS THE SUBJECT OF THE CLAIM IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM

6. Indemnification. In the event that any Third Party should make a claim against either Customer or Company (the "Recipient," which may refer to either Customer or Company depending upon which Party receives the Material), that any information, design, specification, instruction, software, service, data, or material (collectively the "Material") furnished by either Customer or Company (the "Provider," which may refer to either Customer or Company depending on which Party provides the Material), and used by the Recipient infringes on such Third Party's intellectual property rights, the Provider, at its sole cost and expense, shall defend the Recipient against the claim and indemnify the Recipient from any damages, liabilities, costs and expenses awarded by a court of competent to the Third Party claiming infringement or the settlement agreed to by the Provider, provided that the Recipient does all of the following: (A) promptly notifies the Provider in writing, but in no event later than thirty (30) days subsequent to when the Recipient receives Notice of the claim (or sooner if required by applicable law); (B) gives the Provider sole control of the defense and any settlement negotiations; and (C) gives the Provider the information, authority, and assistance the Provider needs to defend against or settle the claim. In the event the Provider believes or it is determined that any of the Material may have violated a Third Party's intellectual property rights, the

Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for its continued use, or in the event that these alternatives are not commercially reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such return materially affects Company's ability to meet its obligations hereunder, then Company may, at its option and upon providing thirty (30) days prior written Notice to Customer, terminate this Agreement. The Provider will not indemnify the Recipient if the Recipient alters the Material or uses it outside the scope of use identified in the Provider's user documentation or services policies or if the Recipient uses a version of the Materials which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was provided to the Recipient. The Provider will not indemnify the Recipient to the extent that an infringement claim is based upon (i) any information, design, specification, instruction, software, data, or material not furnished by the Provider, or (ii) any Material from a Third Party portal or other external source that is accessible to Customer within or from the Service (e.g., a Third Party web page accessed via a hyperlink). Notwithstanding any of the foregoing, Company has no obligation to indemnify Customer in any circumstance where (a) any infringement claim is based upon the combination of any Material with any products or services not provided by Company; (b) any infringement is caused by the actions of Customer against any Third Party if the Service as delivered to Customer and used in accordance with the terms of this Agreement would not otherwise infringe any Third Party intellectual property rights; or (c) any infringement claim is based on (1) a patent that Customer was made aware of prior to the Effective Date of this Agreement (pursuant to a claim, demand, or Notice), or (2) any of Customer's actions occurring prior to the Effective Date of this Agreement. It is the express intent of the Parties that this Section 6 provides each Party's exclusive remedy for any infringement claims or damages.

7. Compliance with Export Laws. The export laws and regulations of the United States as well as other relevant local export laws and regulations may apply to the Service. Customer expressly acknowledges and agrees that (A) to the extent applicable, such export control laws may govern Customer's use of the Service under this Agreement; (B) Customer shall comply with all such applicable export laws and regulations; (C) no data, information, software programs and/or materials resulting from Service (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

8. Force Majeure. Neither Party shall be responsible for any failure or delay in the performance of their respective obligations hereunder provided such failure or delay is caused by a Force Majeure Event; provided, however, that each Party expressly covenants and agrees to use reasonable efforts to mitigate the effect of a Force Majeure Event that should occur during the Term of this Agreement. In the event that a Force Majeure Event occurs and continues for more than thirty (30) days, either Party may cancel any unperformed service upon providing advance written Notice to the other Party.

9. Other Provisions. Time is of the essence of each of the provisions of this Agreement. Customer shall not assign, transfer or encumber this Agreement without obtaining prior written consent of Company, nor shall any attempted assignment, transfer or encumbrance of this Agreement be effectuated by operation of law or otherwise without the prior written consent of Company. Company may assign or transfer this Agreement to any affiliate without obtaining consent from Customer, written or otherwise, and such assignment or transfer shall be effective immediately upon execution and delivery by Company. The Parties hereto expressly acknowledge and agree that, as between the Parties, (A) except as otherwise expressly set forth herein, no representation(s) has been made with respect to the subject matter of this Agreement, nor any representations inducing the execution and delivery of this Agreement; (B) each Party has relied on such Party's own judgment in entering into this Agreement; and (C) any statements and/or representations that may have been made previously by either of them to the other are void and of no effect, and that neither of them has relied upon such statements and/or representations in connection with such Party's dealings with the other. The Parties expressly agree that it is their intention and covenant that

(i) this Agreement constitutes the entire agreement between the Parties regarding the subject matter hereof, and that any and all prior agreements, proposals or communications (whether oral or written) between the Parties are superseded by and merged into this Agreement; (ii) this Agreement, any performance under this Agreement, and all suits and proceedings arising out of, related to, in connection with or by reason of this Agreement between the Parties, be construed in accordance with, and under and pursuant to, the laws of the State of Mississippi; (iii) the laws of the State of Mississippi will be applicable and will govern any action or other proceeding that may be brought by either Party arising out of, related to, in connection with or by reason of this Agreement, to the exclusion of the law of any other forum; (iv) unless expressly waived by Company, the exclusive jurisdiction and venue of any legal action between the Parties with respect to the subject matter of this Agreement shall be the appropriate court(s) in the Southern District of Mississippi; and (v) each of the Parties hereto submits itself to the exclusive jurisdiction and venue of such court(s) for the purpose of any such legal action. If it becomes necessary for any Party to undertake any litigation or to employ an attorney to assist such Party in pursuit of or protection of its rights under this Agreement, the non-prevailing Party shall be obligated to reimburse the prevailing Party for such fees and related costs and expenses, including reasonable attorney's fees, whether incurred at trial, on appeal, or otherwise. The invalidity, illegality, or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if such invalid, illegal, or unenforceable provision had been omitted. This Agreement may be modified or amended by Company from time to time, and where material modifications or amendments are made Company will provide appropriate notice to Customer in such circumstances, whereupon Customer's continued use of the Service will constitute and express acceptance of such modifications or amendments. All terms and conditions of this Agreement shall be binding upon the successors and assigns of the Parties hereto. No waiver of any provision of this Agreement shall be implied by any failure of either Party to enforce any remedy upon the violation of such provision, even if such violation is continued or repeated subsequently. No express waiver shall affect any provision other than the one specified in such waiver, and that only for the time and in the manner specifically stated. Captions to and headings of the Sections and paragraphs of this Agreement are solely for the convenience of the Parties and shall not be used for the interpretation or determination of the validity of the Agreement and/or any provision(s) hereof. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine, neuter, singular or plural as the identity of the person or persons may require. Provisions that survive expiration or termination of this Agreement are those provisions relating to limitation of liability, infringement indemnity and any others which by their nature are intended to survive.

4820-4721-4247, v. 1



iQ2® / iQCommSentry®
WIRELESS SERVICE AGREEMENT No. _____

EXHIBIT "A" (V1) xx/xx/20xx

Business Name
Address
City State Zip
Telephone
Email

Effective Date:

Agreement Term:

Node Summary:

Site	Information

Monthly Charges:

Description	Quantity	Unit Price	Extension

SPECIAL PROVISIONS:

iQ2® / iQCommSentry® WIRELESS SERVICE AGREEMENT

THIS iQ2® / iQCommSentry® WIRELESS SERVICE AGREEMENT (the "Agreement") is made and entered into by and between LEC, INC., a Mississippi Business Corporation (the "Company") and _____, (the "Customer"). Company and Customer may hereinafter be referred to as a "Party" in the singular and the "Parties" collectively.

Section 1. Definitions.

1.1 "Affiliate" of a Party means any entity that controls, is controlled by, or is under common control with, such Party.

1.2 "Acceptable Application" means a software program, application or platform that will be combined with the Service and used by Customer or end users and which is compatible with the efficient operation of the Network, does not interfere with the services of other parties, does not result in inefficient or excessive use of the Network or the networks of Company's roaming carriers, and is not inconsistent with Network policies and practices.

1.3 "Approved Device" means a Device that has been certified and approved by Company.

1.4 "Area(s)" means the areas within the United States where Company is licensed to provide the Service and is providing Service. The Area may change from time to time.

1.5 "Device" means the equipment used by a Customer to originate or receive wireless transmissions on the Network, including any machine to machine communications unit, wireless modem, SIM, and any accessories. Cellular telephone(s) are expressly excluded from this definition.

1.6 "Equipment" means all equipment (other than equipment comprising portions of the Network) necessary to enable Customer to use or benefit from the Service, including but not limited to Customer's network facilities and any Device.

1.7 "Events of Default" means the following: (i) the execution of any assignment for the benefit of creditors or the filing for relief by either Party under any applicable bankruptcy, reorganization, moratorium, or similar debtor relief; (ii) the appointment of a receiver for Customer or Company or for substantially all of their respective assets or properties; (iii) Customer's failure to pay any sum owed to the other hereunder at the time such amount comes due; (iv) either Party's failure to perform or observe any other term, condition, or covenant to be performed by it under this Agreement; (v) an unauthorized assignment of this Agreement; or (vi) Customer's failure to utilize Equipment compatible with the Network or other network of Company, as determined by Company.

1.8 "Hosting Services" means access to the iQ2® / iQCommSentry® interface (as applicable), together with certain additional related services which may include private cellular network access, periodic firmware upgrades to the Service Devices (when necessary), temporary storage of Customer data, hosting of Customer remote-site web pages(s) (when applicable), remote troubleshooting, user-access management, carrier support and twenty-four (24) hour customer service. In certain cases, Hosting Services may also include custom Virtual Private Network configuration and maintenance, content filtering, usage monitoring and limiting, data pooling, network architecture and configuration assistance, transmission of data log(s) to Customer, site-to-site communication and alarm messaging.

1.9 "Machine to Machine Communications" means wireless communications made possible by the provisioning of an Approved Device or the insertion of a SIM by Customer or its agent into an Approved Device (as applicable) for use with an Acceptable Application upon activation of the Service, for use by Customer.

1.10 "Network" means those integrated mobile switching facilities, servers, cell sites, connections, billing systems and other related facilities used by Company to provide Service in an Area.

1.11 "Service" means the Hosting Services, and any machine to machine data and SMS wireless telecommunications services (as and where available) for GSM communications, GPRS (General Packet Radio Services), EDGE, Universal Mobile Telephone Service (UMTS), High Speed Packet Access (HSPA) Service, High Speed Packet

Access + (HSPA+), Code Division Multiple Access Service (CDMA), Enhanced Voice-Data Optimized Service (EVDO) or Long Term Evolution (LTE) technology. Service does not include any voice service.

1.12 "Service Plan" means the particular set of rates, terms and conditions as stated in the Exhibits to this Agreement upon which Company makes Service available to Customer, but does not include any short-term marketing promotions that may periodically be offered by Company.

1.13 "Subscriber Identity Module ("SIM")" means a specially programmed microchip that is inserted into a Device which encrypts transmissions and identifies the user to the Network.

1.14 "Subscription Fraud" means using or assisting another to use any scheme, false representation, or false credit device, or other fraudulent means or devices in connection with Service or any Service Device.

1.15 "Unauthorized Access" means any unauthorized use of the Service or any Service Device, which includes the practices generally referred to as "counterfeiting," "cloning fraud," or "tumbling fraud."

TERMS AND CONDITIONS

Section 2. Purchase and Sale of the Service. Customer agrees to purchase from Company, and Company agrees to sell to Customer, the Service for use in Machine to Machine Communications on Company's wireless Network as stated in the Exhibits hereto. The Service is provided to Customer for Customer's use and not for resale. The Service (other than roaming service) is only available in the Area. At all times Customer will comply with Company policies and procedures reasonably established by Company for providing the Service, and Company may from time to time modify these policies and procedures.

Section 3. Term. This Agreement commences on the Effective Date and remains in effect for the length of the Agreement Period as both are identified in Exhibit A attached hereto and incorporated herein by reference (the "Term"). This Agreement will automatically renew for successive one (1) year renewal Term(s) unless either Party provides the other with a notice of termination at least thirty (30) days prior to the end of the then-current Term.

Section 4. The Service.

4.1 Network Connections. Customer must connect to the Network in order to receive the Service. Such connections may be obtained under this Agreement or pursuant to separate agreement between the Parties.

4.2 General Service Requirements. Company will only activate Service for use with the Acceptable Applications and Approved Device(s). Company may require a minimum number of Device(s) to be activated at one time. To the extent that SIMs are required for Service, Customer is only authorized to purchase SIMs directly from Company or through Company's Affiliate(s) for use on the Network. Unless otherwise stated, an Approved Device, an Acceptable Application(s) and a SIM (when applicable) are required for all Service Plans. Company may, at its option, require Customer to provide information about how their applications interact with the Network, and may limit, restrict or prohibit use of applications in Company's sole discretion.

4.3 Service Requiring Use of SIMs. A number may not be associated with more than one SIM at the same time, unless otherwise approved by Company. Company may deny Service to any SIM(s) without liability to Customer for SIMs appearing on Company's service deny lists for reasons including, but not limited to, cases where the SIM is stolen, has been used for fraudulent purposes, is not used in an Approved Device or with an Acceptable Application, or is defective, and Company will notify Customer in such cases. Customer must not insert any SIM into anything other than an Approved Device, and/or program, re-program or tamper with any SIM in any manner, and Customer shall be responsible for the payment of any and all charges incurred resulting from any violation of this Agreement.

4.4 Modification or Termination of Service. If Customer desires to modify or terminate any Service or change Service Plans, Customer must advise Company in writing accordingly. Changes will become effective as determined by Company. Should Customer terminate Service under this Agreement at any time during the Term (or any renewal thereof as provided in Section 3), Customer shall pay to Company an early termination fee in an amount equal to fifty percent (50%) of the total balance of the Service Plan for the remaining current Term.

4.5 Troubleshooting. Customer will cooperate with Company in any troubleshooting of the Equipment or the Network as required to maintain the efficient operation of the Service.

4.6 Limitations on Roaming Service.

4.6.1 THE AVAILABILITY OF ROAMING SERVICES, AND THE CHARGES FOR THOSE SERVICES, IS DEPENDENT IN PART ON THE TYPE OF EQUIPMENT USED BY CUSTOMER AND THE PROGRAMMING OF THAT EQUIPMENT. COMPANY MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE AVAILABILITY OR QUALITY OF ROAMING SERVICE PROVIDED BY OTHER WIRELESS NETWORKS, AND COMPANY WILL NOT BE LIABLE IN ANY CAPACITY FOR ANY ERRORS, OUTAGES, OR FAILURES OF ROAMING SERVICES PROVIDED BY OTHER WIRELESS NETWORKS.

4.6.2 IF COMPANY, OR ANOTHER ENTITY WITH WHOM COMPANY HAS A ROAMING AGREEMENT, DISCOVERS OR SUSPECTS ABUSE OR FRAUD WITH RESPECT TO CERTAIN NUMBERS, THEN ROAMING PRIVILEGES MAY BE SUSPENDED WITH RESPECT TO SUCH NUMBERS. COMPANY WILL USE COMMERCIALY REASONABLE EFFORTS TO PROVIDE CUSTOMER WITH PRIOR, OR PROMPT SUBSEQUENT, NOTIFICATION OF THE SUSPENSION OF THE ROAMING SERVICE. COMPANY WILL NOT BE LIABLE IN ANY CAPACITY TO CUSTOMER FOR THE UNAVAILABILITY OR SUSPENSION OF ROAMING SERVICE BY OTHER CARRIERS.

4.6.3 TO THE EXTENT ACCESS TO ROAMING CAPABILITIES IS PROVIDED BY COMPANY TO CUSTOMER, IT IS DEEMED TO BE A "SERVICE" AS DEFINED IN SECTION 1, AND THE USE OF SUCH ROAMING BY CUSTOMER WILL BE GOVERNED BY THE PROVISIONS OF THIS AGREEMENT.

4.7 Service Technology Disclosures. The underlying carrier is not obligated to maintain any particular technology, and Network technologies may be terminated at any time in its sole discretion. Company will provide Customer twelve (12) months prior written notice of any termination of a significant wireless technology on a nationwide basis.

4.8 International Roaming. Service is not permitted to be used under this Agreement for international roaming, except on a rare and incidental basis. Should Company, in its sole discretion, determine that Customer is utilizing international roaming more frequently than on a rare and incidental basis, Company may terminate such international roaming with or without notice to Customer of such termination. With respect to any international roaming under this Agreement, Customer (i) shall provide Company with all assistance reasonably required to enable Company to comply with requests or requirements of a roaming carrier, regulator, or other governmental body relating to Customer's use of international roaming; (ii) shall comply with each country's legal and regulatory requirements arising from or relating to Customer's use of the Service; (iii) shall provide Company with the place of primary use of the Service (which must be its business street address and be within an eligible Company wireless Service area); (iv) expressly acknowledges that Service may not be available outside of a provisioned roaming zone; and (v) shall indemnify and hold Company harmless from any claims, costs, losses or damages resulting from Customer's international roaming.

4.9 PRIVACY. THE NETWORK HAS MANY COMPLEX ELEMENTS AND IS NOT GUARANTEED AGAINST EAVESDROPPERS, HACKERS, DENIAL OF SERVICE ATTACKS, VIRUSES, OR INTERCEPTORS. CUSTOMER AGREES THAT COMPANY WILL NOT BE LIABLE TO CUSTOMER OR TO END USERS FOR ANY LACK OF PRIVACY OR SECURITY. IN THE EVENT THAT CUSTOMER SUBSCRIBES TO AN UNMANAGED SERVICES PLAN, CUSTOMER EXPRESLY ACKNOWLEDGES AND AGREES THAT CUSTOMER SHALL BE SOLELY REPONSIBLE FOR ANY AND ALL SECURITY AND DATA MONITORING ASSOCIATED WITH SUCH SERVICE PLAN.

Section 5. DISCLOSURE AND ACKNOWLEDGMENT. CUSTOMER UNDERSTANDS AND AGREES (I) THAT CUSTOMER HAS NO CONTRACTUAL RELATIONSHIP WITH THE UNDERLYING WIRELESS SERVICE CARRIER/PROVIDER; (II) THAT CUSTOMER IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN COMPANY AND THE UNDERLYING CARRIER/PROVIDER; (III) THAT THE UNDERLYING CARRIER/PROVIDER HAS NO LEGAL OR EQUITABLE LIABILITY OF ANY KIND TO CUSTOMER WHATSOEVER, WHETHER FOR BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE, AND CUSTOMER HEREBY WAIVES ANY AND ALL CLAIMS OR DEMANDS THEREFORE; (IV) THAT MESSAGES MAY BE DELAYED, DELETED OR NOT DELIVERED; AND (V) THAT THE UNDERLYING CARRIER CANNOT GUARANTEE THE SECURITY OF WIRELESS TRANSMISSIONS AND WILL NOT BE LIABLE FOR ANY LACK OF SECURITY RELATING TO THE USE OF THE SERVICES.

Section 6. Rates.

6.1 Service Plans. Customer will pay for Service at the rates set forth in the applicable Service Plan(s) as selected by Customer. Rate plan changes will take effect as stated in the Exhibits. Company may modify a Service Plan or charge at any time by providing thirty (30) days advance written notice to Customer, provided that any modification not adverse to Customer may be made immediately effective upon written notice.

6.2 Service Outages. In the event of a total Service outage within an Area which is not caused by Customer and which lasts for a period of twenty-four (24) hours or more, a credit allowance will be made at Customer's request in the form of a pro rata adjustment of the fixed charges billed by Company to Customer with respect to the affected SIM(s). Periods of discontinuous outage may not be accumulated in determining if an outage has continued for at least twenty-four (24) hours. In order to receive such credit, Customer must submit a written request to Company, stating the date and location of the outage, the SIMs affected, and such other information as Company may reasonably require. Such notice must be received by Company within ten (10) business days following the last date of the period of outage. EXCEPT AS PROVIDED HEREIN, COMPANY WILL NOT INCUR ANY LIABILITY OF ANY NATURE OR TYPE WHATSOEVER FOR SERVICE OUTAGES.

Section 7. Invoices, Payments, Disputed Charges and Billing Data.

7.1 Invoices and Billing Data. Company will provide Customer a summary invoice for all charges on a monthly basis, normally within ten (10) days subsequent to the cut-off date for each billing cycle, each such invoice containing all charges and applicable taxes and/or regulatory fees. All SIMs will be placed on the same billing cycle. Customer must notify Company if Customer has not received an invoice within twenty (20) days subsequent to the bill cycle cut-off date. Company will use reasonable efforts to provide electronic detailed billing data for all Service Plans loaded into a billing cycle.

7.2 Payments. Payment in full for each invoice is due at the location set forth in the invoice, in a form payable in U.S. currency, upon the due date set forth in the invoice or within thirty (30) days subsequent to receipt of the billing data (which shall include any amounts due for data usage in excess of the allotted amount for the then-current billing period), whichever is later (the "Due Date"). For purposes of payment, Customer may rely only on the invoice and other billing data received from Company, and may not rely on any other source including information drawn from any Company or Customer system. Depending on Customer's payment history, Company may at its sole discretion require payment by certified check, money order, or wire transfer. Payments are past due, and Customer will have committed an Event of Default, if not received by the Due Date. Time is of the essence with respect to payment of Company's invoices. If a payment becomes past due, the account will accrue late fees and interest at the rate of one and one-half percent (1.50%) per month or the maximum lawful rate, whichever is greater. Customer agrees not to place any condition or restrictive legend, such as "Paid in Full", on any check or financial instrument used to make a payment. The Parties agree that the negotiation of any such check or instrument so inscribed will not constitute an accord and satisfaction or novation.

7.2.1 Suspension of Service. In the event that Customer fails to timely make payments to Company as required in this Agreement, Company may suspend the Service at any time. During the pendency of any suspension of Service, all charges, fees and taxes for Service will continue to accrue, and Customer will continue to be financially responsible for the payment of such amounts. In order to restore any suspended Service, Customer shall pay a reactivation fee in the additional amount of One Hundred United States Dollars (\$100.00) per Device.

7.3 Disputed Charges. If Customer disputes part of the monthly invoice, Customer is required to notify Company in writing and to submit appropriate documentation justifying such dispute to Company as soon as it is aware of the dispute, but in no event later than the thirty (30) days after the invoice Due Date or such dispute is waived. Notwithstanding any such dispute, Customer agrees to pay the full amount of any such bill pending the resolution of such dispute. Company will respond to Customer's written dispute within thirty (30) days of receipt of such dispute. Company and Customer agree to use best efforts to resolve all disputes and Company agrees to promptly refund any amounts due upon dispute resolution. The notice requirements in this Paragraph 7.3 will not shorten the period within which actions must be filed as established by the applicable statute of limitations, but will constitute a condition precedent to any right of the aggrieved Party to contest prior invoices or payments. This condition is designed to allow each Party the opportunity to preserve important evidence in defense of a claim.

Section 8. Abusive or Fraudulent Use.

8.1 Generally. Service may be restricted or cancelled if there is a reasonable suspicion of abuse or fraudulent use. Company will provide prompt notice of the restriction or termination to Customer. Customer agrees to make good faith efforts to minimize abuse or fraudulent use, to promptly report to Company any such abuse or fraudulent

use of which Customer becomes aware, and to cooperate in any investigation or prosecution initiated by Company. Customer also agrees that Company may in its discretion disable any Device, or otherwise block access to the Service when suspected of abuse or fraudulent use. Abuse and fraudulent use of Service include, but are not limited to (i) attempting or assisting another to access, alter, or interfere with the communications of and/or information about another wireless customer; (ii) tampering with or making an unauthorized connection to the Network; (iii) installing any amplifiers, enhancers, repeaters, or other devices that modify the radio frequencies used to provide the Service; (iv) Subscription Fraud; (v) using Service in such a manner so as to interfere unreasonably with the use of Service by one or more other wireless customers or to interfere unreasonably with Company's ability to provide Service; (vi) using Service to convey obscene, salacious, or unlawful information; (vii) using Service without permission on a stolen or lost Device; (viii) Unauthorized Access; (ix) using the Service to provide voice over IP services; and/or (x) extensive use of the Service outside of the Area.

8.2 Liability for Abuse or Fraudulent Usage. Customer is solely liable for charges, costs and damages resulting from (i) Subscription Fraud, (ii) any theft of a Device, any user identification number, or password associated with the Service; (iii) any abuse or fraud facilitated by Customer, Customer's employees, or Customer's agents, and/or (iv) any failure to give prompt notice of suspected abuse or fraudulent use based on information available to Customer.

Section 9. Limitation of Liability.

9.1 Generally. COMPANY'S ENTIRE LIABILITY, AND CUSTOMER'S EXCLUSIVE REMEDY, FOR DAMAGES ARISING OUT OF MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, LOSS OR CORRUPTION OF CUSTOMER'S DATA, ERRORS OR DEFECTS IN THE SERVICE(S), SHALL IN NO EVENT EXCEED THE SPECIFIED CREDITS UNDER THIS AGREEMENT, OR IF NO CREDITS ARE SPECIFIED, AN AMOUNT EQUIVALENT TO THE PROPORTIONATE CHARGE TO CUSTOMER FOR THE PERIOD OF SERVICE DURING WHICH SUCH MISTAKE, OMISSION, INTERRUPTION, DELAY, ERROR OR DEFECT IN THE SERVICES OCCURS AND CONTINUES. IN NO EVENT SHALL ANY OTHER LIABILITY ATTACH TO COMPANY.

9.2 Consequential Damages. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES, OR INCREASED COST OF OPERATIONS.

Section 10. Default and Termination.

10.1 Default. This Agreement may be terminated upon an Event of Default by either Party if such Event of Default is not cured by the defaulting Party within thirty (30) days subsequent to receipt of a notice of the Default; provided, however, that in the case of failure to pay invoices or in the case of a violation of Section 8 of this Agreement, this Agreement may be terminated if such Event of Default is not cured within ten (10) days subsequent to receipt of notice of the Event of Default.

10.2 Termination for Convenience. Company may terminate this Agreement at its convenience upon ninety (90) days' prior written notice to Customer.

Section 11. Installation Services Warranty. The Installation Services Warranty applies to all work performed by Company in connection with the establishment of the Service (the "Installation Services"). Company warrants and represents that the Installation Services shall be free from any material defect for a period of one (1) year subsequent to the commencement of the initial Term of this Agreement (the "Installation Services Warranty Period"). In the event that Customer notifies Company during the Installation Services Warranty Period that a defect in the Installation Services exists, Company agrees to provide such services as are reasonably necessary to correct said defect in the Installation Services at no cost to Customer; provided, however, that in the event Company in good faith determines that the alleged defect is not due to any fault of Company, or if Customer's notice is tendered subsequent to the expiration of the Installation Services Warranty Period, then Customer shall pay Company for all services provided to Customer in accordance with Company's then-current rate schedule. The Installation Services Warranty only applies to defects in the Installation Services and not defects in any Device(s) or Equipment, or defects caused by other circumstances, including without limitation accident, misuse, unforeseeable use, neglect, alteration, vandalism, improper installation by others, improper testing, improper repair and/or Acts of God.

Section 12. Other Provisions. All notices and other communications under this Agreement shall be in writing and shall be deemed given when delivered personally, transmitted by facsimile (provided that a copy of such facsimile is sent by certified mail, return receipt requested) or sent by certified mail, return receipt requested, to the Parties

address(es) of record. Time is of the essence of each of the provisions of this Agreement. Customer shall not assign, transfer or encumber this Agreement without obtaining prior written consent of Company, nor shall any attempted assignment, transfer or encumbrance of this Agreement be effectuated by operation of law or otherwise without the prior written consent of Company. Company may assign or transfer this Agreement to any Affiliate without obtaining consent from Customer, written or otherwise, and such assignment or transfer shall be effective immediately upon execution and delivery by Company. The person executing this Agreement on behalf of Customer expressly warrants and represents that he/she is the authorized representative of Customer and possesses the requisite authority to legally bind Customer to the terms and conditions hereof. The Parties hereto expressly acknowledge and agree that (i) except as otherwise expressly set forth herein, no representation(s) has been made with respect to the subject matter of this Agreement, nor any representations inducing the execution and delivery of this Agreement, (ii) each Party has relied on such Party's own judgment in entering into this Agreement, and (iii) any statements and/or representations that may have been made previously by either of them to the other are void and of no effect, and that neither of them has relied upon such statements and/or representations in connection with such Party's dealings with the other. The Parties expressly agree that it is their intention and covenant that (A) this Agreement, any performance under this Agreement, and all suits and proceedings arising out of, related to, in connection with or by reason of this Agreement, be construed in accordance with, and under and pursuant to, the laws of the State of Mississippi; (B) the laws of the State of Mississippi will be applicable and will govern any action or other proceeding that may be brought arising out of, related to, in connection with or by reason of this Agreement, to the exclusion of the law of any other forum; (C) unless expressly waived by Company, the exclusive jurisdiction and venue of any legal action with respect to the subject matter of this Agreement shall be the appropriate Court for Rankin County, Mississippi, and (D) each of the Parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such legal action. If it becomes necessary for any Party to undertake any litigation or to employ an attorney to assist such Party in pursuit of or protection of its rights under this Agreement, the non-prevailing Party shall be obligated to reimburse the prevailing Party for such fees and related costs and expenses, including reasonable attorney's fees, whether incurred at trial, on appeal, or otherwise. The invalidity, illegality, or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if such invalid, illegal, or unenforceable provision had been omitted. This Agreement shall not be amended or modified, and none of the provisions hereof shall be waived, except in a writing signed on behalf of the Parties hereto or, in the case of a waiver, on behalf of the Party making the waiver. All terms and conditions of this Agreement shall be binding upon the successors and assigns of the Parties hereto. No waiver of any provision of this Agreement shall be implied by any failure of either Party to enforce any remedy upon the violation of such provision, even if such violation is continued or repeated subsequently. No express waiver shall affect any provision other than the one specified in such waiver, and that only for the time and in the manner specifically stated. This Agreement may be executed in any number of copies, each of which shall be deemed an original and no other copy need be produced. Captions to and headings of the Sections and Paragraphs of this Agreement are solely for the convenience of the Parties and shall not be used for the interpretation or determination of the validity of the Agreement and/or any provision(s) hereof. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine, neuter, singular or plural as the identity of the person or persons may require.

COMPANY:

CUSTOMER:

LEC, INC.

A Mississippi Business Corporation

Name of Company



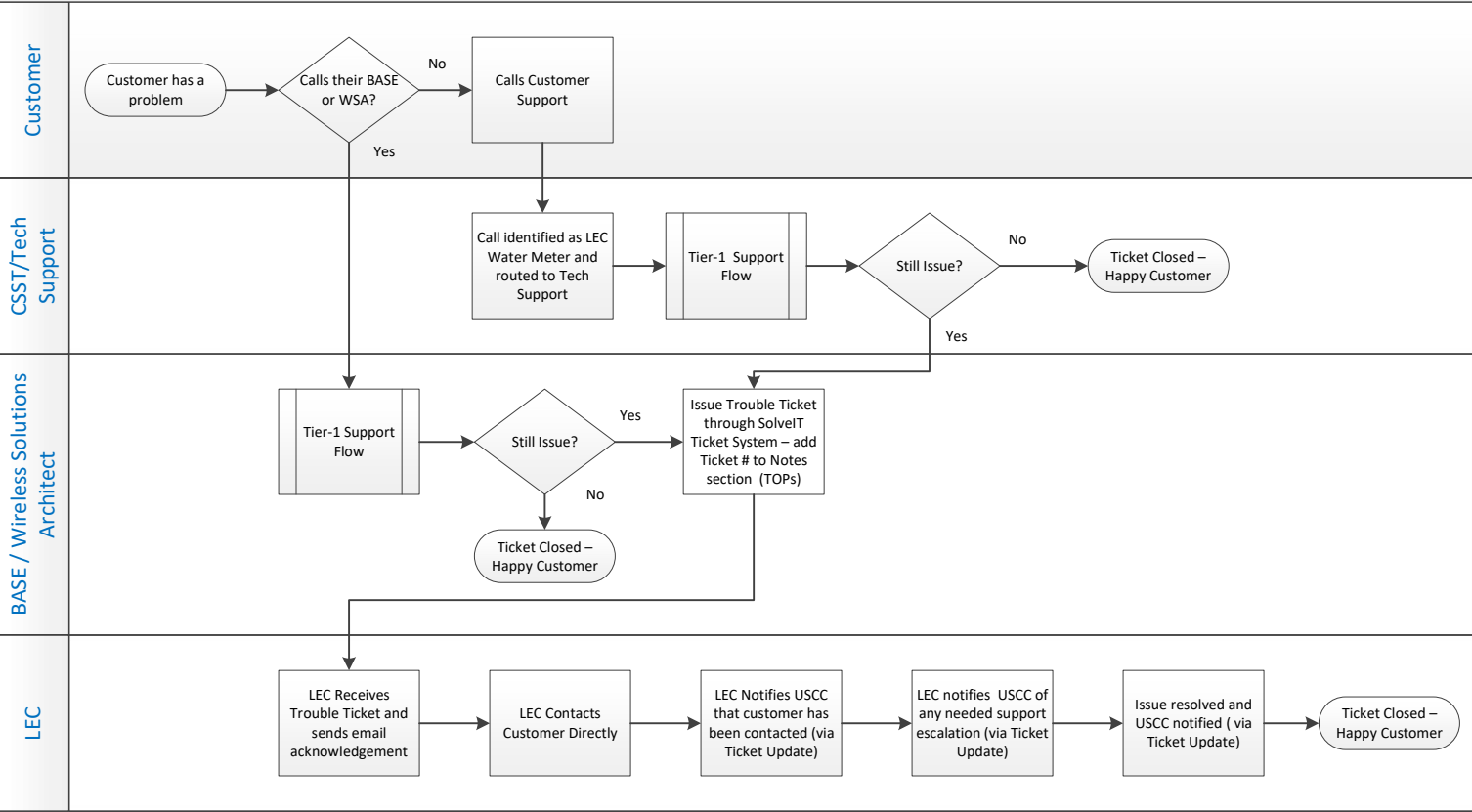
By: _____
Authorized Representative
(Signature)

Authorized Representative
(Signature)

Title

Smart Water Meter Cellular Endpoint - Troubleshooting

Phase



Leaders In Industrial Automation Control Engineering and IIoT Communication



Leaders in Industrial Automation
Control Engineering and
IIoT Communication



Our Applications

In the ever-evolving motion-control and electric motor industry, LEC's international experience in developing components, engineering systems and programming software for clients spans a vast array of verticals. Our broad client portfolio ranges from oil & gas, pipeline and transportation companies to water/wastewater, forestry and many more key industries.



Oil & Gas, Pipeline

- Drilling Rig Remote Monitoring Systems
- Production Monitoring Systems
- Pumping Unit Monitoring Systems
- Pipeline Metering Station Monitoring and Control Systems
- Pipeline Control and Block Valve Controls and Monitoring Systems
- Pipeline SCADA Systems



Water / Wastewater

- Wastewater Pump Stations
- Potable Water Well Controls
- Elevated Tank Controls
- Treatment Process Controls



Metals & Machining

- C-N-C Machining
- Arc Furnaces
- Punch Presses
- Rolling/Stamping/Slitting
- Die Casting
- Draw Blocks
- Annealing



Forestry / Agriculture

- Bucking, Sawing & Chipping
- Trimming, Sorting & Stacking
- Drying & Packaging



Power Generation

- Fuel Tank Farm Supervisory Control
- Process Water Filtration & Treatment
- Wastewater Filtration & Treatment
- Electrostatic Precipitator Controls
- Bottom Ash Control Systems
- Fly Ash Control Systems
- Hydro-Electric Generator Controls
- Raw Water Intake Controls



Robotics

- Pick & Place
- Welding
- Assembly



Communications

- Ethernet Networks
- VPN Access
- ControlNET
- DeviceNET
- Modbus / RS485
- Fiber Optic
- Cellular
- Internet



Monitoring

- SCADA Systems
- Remote Monitoring Systems
- Residual Chlorine Monitoring Systems



Automotive

- Tire Industry
- Welding Machines
- Component Assembly
- Automation
- Quality Control - Vision
- Inspection Systems



Plastics

- Injection Molding
- Extruding
- Blow Molding
- Thermoforming
- Ultra-Sonic Welding



Food & Beverage

- Batching
- Ovens
- Fillers/Seamers/Cappers
- Packaging
- Palletizers
- Bar Coding/Sorting



Chemical

- Custom Container Filling Stations
- Palletizers
- Batch Controllers



Paper Industry

- Paper & Pulp
- Converting
- Presses



Fiber Glass Insulation Production

- SMC Production
- 10 & 15 Ton Presses



Transportation

- Draw Bridge Controls
- Bridge Automation



Amusement & Entertainment

- Roller Coaster Automation
- Water Park Automation

LEC Is Engineering Smarter Systems

LEC supplies the competitive advantage to industry, turning challenging circumstances into revenue-generating results by providing the cutting-edge production and process management automation tools needed to face competitors head-on in a demanding global marketplace. Our proven experience is demonstrated via our clients' success in areas such as cost reduction, higher-quality manufacturing, process efficiency increase, greater employee safety and productivity improvement.



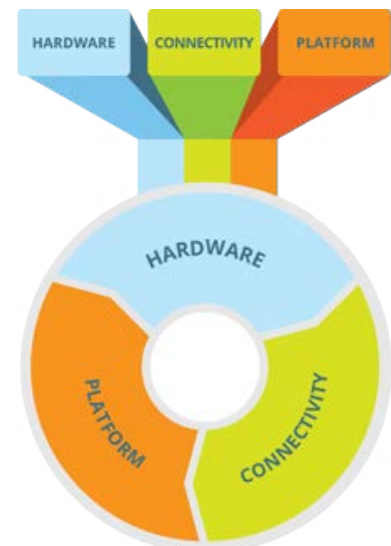
Who We Are

LEC provides industrial automation and control engineering, and industrial IIoT enablement and cloud platform services of the highest quality. Every day, we demonstrate an unending commitment to our clients, strategic partners and communities.

Automation is a crucial element of the manufacturing and production process. The efficiency of any process is dependent on successful system integration. LEC supplies the competitive advantage to industry, turning challenging circumstances into revenue-generating results. We provide the cutting-edge production and process management automation tools needed to face competitors head-on. LEC produces tangible benefits - cost reduction, higher-quality manufacturing, process efficiency increases, greater employee safety and productivity improvement.

Access to our professionals is not restricted to "traditional" business hours and workdays. Our highly experienced emergency support teams are available any time – day or night. By incorporating remote access features into your control system, our teams are enabled to diagnose issues, and in many cases remedy them from virtually anywhere.

Additionally, we offer our clients the option of attending customized training sessions, either on-site or in a hands-on classroom environment.



Proven Industry Leaders

Our passion is engineering smarter systems that exceed expectations. LEC's experienced and passionate team brings a multidisciplinary approach to addressing the challenges that affect our clients. We're setting a new standard in industrial automation control engineering and IIoT enablement.



Strategic Partner Alliances

LEC's well-established strategic alliances with industry leading component manufacturers, hardware providers, network carriers and platform developers enable our team to successfully design, produce, and integrate custom systems based on the specific, individual needs of each client. These Alliances play a vital role in LEC's consistent delivery of successful results.

Experienced Human Resources Behind the Technology

The core of our flexible workforce includes engineers experienced in a variety of disciplines with the knowledge to complete a project of any size and in nearly any industrial application. Our professionals are passionate about design, fluent with technology, and engaged in each aspect of every project.

- Automation Engineers
- Industrial Engineers
- Network Architects
- Electrical Engineers
- Mechanical Engineers
- Computer Engineers
- Civil Engineers
- Network Engineers
- PLC/Automation Programmers
- Certified Panel Technicians



Engineering Products & Services

Engineering & Consultation

Consulting services offered by LEC range from specification of a single system component to turnkey design-build services. We have an extensive network of resources, both technical and non-technical, which allows us to accommodate client needs during any phase of a project. These services are not specific to any particular market segment and are applicable to both public and private-sector projects. LEC provides the solutions needed as well as the documentation required to keep up with all details of a project; including schematics, hardware/software manuals, and fabrication details. All of our documents are accurate, easy to follow, and simple to modify.



Industrial Automation & Control Systems

LEC's team has decades of experience in engineering smarter automation systems for industry, delivering real solutions to successfully solve critical process and control application challenges. We are committed to the continuous training of our team and to the innovation advancement of our industrial automation services. Whether you need a single-station work cell, a completely integrated multi-functional assembly line, or the integration of new components into an existing system, LEC has the solution. Our team of experienced engineers, programmers, technicians, and software developers focuses on providing cost-effective solutions. Clients rely on us for process integration, machine design and build, PLC and RTU programming, HMI SCADA development, production monitoring and reporting, data collection, servo and VFD programming, machine diagnostics and alarming, panel design, and industrial IoT solutions.

Systems Integration

LEC's experienced team of control system integrators design and implement sophisticated control systems for manufacturing operations, process and other industrial facilities. We leverage our extensive knowledge of engineering, information technology, operations, and business to expertly integrate plant equipment to automate manufacturing and processes from the plant floor to the enterprise level. Automation helps manufacturers and processors reduce cost, increase production, use less energy and lower environmental impact. Our extensive experience with a vast array of hardware and software platforms and their unique communication protocols enables us to effectively integrate multiple machine control systems in accordance with specific client requirements, whether into a comprehensive control room, SCADA application, or cloud-based solution.



Engineering Products & Services

UL-508A Certified Industrial Panel Design & Fabrication

LEC specializes in providing custom control panel solutions of the highest caliber in the manufacturing industry with a proven track record of satisfying a variety of industrial automation needs. Our team of highly experienced technicians expertly construct control panels to the highest quality of industry standards using the best products from trusted hardware manufacturers. LEC's UL-508A Certified Panel Shop can accommodate any size project, and provide engineering support from design concept to completion.



Skid Design & Fabrication

Our engineers, technicians and fabrication teams provide the best quality skid-mounted measurement technologies and mechanical and electrical controls available in the industry. LEC's professionals can manage and advise on your project from initial design through start-up and commissioning. We offer both standard designs for quick turnaround to meet tight deadlines, and customizable solutions to meet unique regional or application requirements.



Programming

PLC Programming

Our skilled professionals provide software programming services for a variety of brands of Programmable Logic Controllers (PLCs). Our software development outcomes are easy to use, organized, and simplified, with descriptive comments to give our clients the information they need to maintain their equipment.

HMI & Operator Interface Programming

Regardless of the complexity of your HMI needs, LEC provides sophisticated, user-friendly systems that are easy to operate, and our professionals are experienced in designing and programming a wide variety of operator interface systems.

Motion Control Programming

We are skilled in the design, installation, and commissioning of an extensive array of motion-control components and variable speed drives, which provide smooth operation of electronic gearing, contouring, and circular motion applications.



Radio Frequency Controls

LEC has extensive experience in providing solutions utilizing a variety of wireless controls and I/O devices in accordance with your particular requirements. These are crucial when an application involves potentially dangerous machinery (such as conveyors and blenders) or the monitoring of equipment, motors and other devices from a remote location.

Programming

Industrial Internet of Things Enablement Products and Services

LEC offers experienced Industrial Internet of Things (IIoT) enablement, filling the gaps between disparate technologies.

- Integrating existing field devices and assets into a current IIoT framework.
- Connecting disparate systems into a single platform and user interface for monitoring and control.
- Developing ground-up, custom IIoT solutions to meet specific client requirements.
- Long-term solution support to ensure sustainability while meeting ongoing and future IIoT business needs.



Mission Critical IIoT Connectivity

- Highly secure and redundant wireless connectivity
- Advanced private network with client access to real-time network analytics
- Managed services staffed with skilled support and troubleshoot personnel
- Pre-commissioned hardware for optimized deployments
- 4G LTE Network
- System Consulting & Design
- Robust 24/7 ticketing system with solveIT™ support tool



Engineering the Components of IIoT

LEC offers experienced Industrial Internet of Things (IIoT) enablement, filling the gaps between disparate technologies. With years of industrial controls and automation experience, along with investment in new and innovative technologies and the brightest human resources, LEC is truly a market leader in deploying IIoT. Trusted by the industry, wireless carriers and enterprise clients alike, LEC is a proven partner in business.

Visualization & Control Through Robust IIoT Platform Technologies

- IIoT platforms delivering data visualization, analytics, and control
- Reliable alarm and fault notification systems
- Ability to extract data and enable control both remotely and in-plant
- Data logging and reporting functionality
- Simple configuration and intuitive user interface
- Access from any browser-enabled device



Introducing iQ2™. Intelligence. Squared.

iQ2 is LEC's complete, end-to-end IIoT platform solution, designed from an industrial automation engineering perspective, to effectively and efficiently address individual needs. Our flexible IIoT integration process quickly and easily enables our cutting-edge platform technology on the plant floor, for OEMs and any industrial remote assets.



ENABLING IIoT

Engineering the Components of IIoT



iQ Web SCADA

LEC's complete end-to-end monitoring and control solution, iQ Web SCADA, integrates into almost any new or existing control or automation system regardless of the function of the machinery, equipment, or system. The iQ Web SCADA platform can be used all or in part, depending on the needs of the user.



iQ CommSentry

LEC's iQ CommSentry service tool provides users with a simple solution to monitor and manage network performance resulting in reduced downtime and the prevention of costly errors. This platform simplifies compliance management, IP address management, easily tracks and locates network users and devices, and analyzes network traffic and bandwidth usage.



COMMSENTRY
MANAGING IIoT

Support



Technical Support Center

LEC's newly-launched, cutting-edge solveIT™ Technical Support Center provides clients with direct, 24/7 access to data, project information and support request updates using the latest technology compatible with today's browsers and mobile devices. solveIT™ is a user-friendly and highly-collaborative cloud-based system designed to give clients instant access to detailed information regardless of locale. solveIT™ features data sharing, client data input capabilities, support ticket tracking, project tracking, hardware information and much more, increasing overall project management effectiveness.

On-Site Support

Technical support is a crucial component of LEC's services, and we are always pleased to assist clients with on-site questions or maintenance needs.



Replacement Components

We have a commitment to providing every nature of support for our clients' systems throughout their service life. In addition to our remote assistance and on-site support services, we also offer replacement components for every aspect of control and automation systems.



**Leaders in Industrial Automation
Control Engineering and
IIoT Communication**

Appendix AA

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory O: Utility Operations, Monitoring and Support

LEC



NASPO
ValuePoint



1 - General information:

Please provide a general description of the solution you are offering including:

- a. Product Name
iQ Pulse- Advanced Metering Infrastructure (AMI)
- b. General Application Area
Subcategory O: Utility Operations, Monitoring and Support
- c. General capabilities provided
The iQ Pulse IIoT Web portal is a water usage collection database that collects and calculates daily water consumption, as well as provides alarming notification mechanisms for detecting slow and fast leaks, high consumption, etc. The data accumulated within the portal is received from a cellular endpoint residing in the field.
- d. Expected impact on cost/performance/functionality, etc.
 - Improved customer service with a detailed capture of usage such as spikes and interruptions that may identify leaks.
 - Reduced truck-rolls to remote sites and infrastructure reduces costs and increases safety
 - Provide real-time and historical data analytics to improve operational efficiency and reduce related costs
 - The cloud-based application provides real-time insight into asset performance via any web-enabled device or handset decreasing response time to critical field failures.
 - Highly flexible system allows low-cost and simple integration with existing systems.
 - Non-proprietary hardware allows for quick availability and competitive costs on off-the shelf hardware across multiple OEM's.
 - Future Proof- Designed and interoperable with systems added later
 - Resilient- cellular service is one of the first systems to be restored so once it is up and running the water meter data is flowing and repopulating readings captured during downtime
- e. Subcontractors/partners involved in delivering service
UScellular partners with LEC to provide this solution.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes, see attached.

2 - Turnkey Wireless Solutions:

Offerors shall fully describe each turnkey system offered in each subcategory. Each offering will be scored based on the perceived value of the turnkey system offered within the subcategory.

- a. Strength and functionality of operational product as described
 - Ease of access to monthly billing data increases revenue stream to municipality and reduces the amount of uncollectable Accounts Receivable
 - Standalone unit with up to 10 years of service with the changeable battery
 - User interface via secure web browser to cloud based portal
 - Access from any device including smartphones and tablets
 - Automated billing troubleshooting and analyzing

- Alert/Alarm functionality including all consumption, diagnostic and meter status indicators
 - Customer access to their secure data available upon request
- b. Applicability to government needs
This remote monitor and control technology supports a broad application and many different use cases.
- c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.
Provide references
Deployed nationwide to multiple municipalities.

IIoT water/wastewater market

Ronnie Jones
Aqua Products, Inc
Sarasota, FL 32505
850-469-1133

- d. Overall interoperability of turnkey system for government use
- Hardware is agnostic to meters in use. Endpoints are validated to run multiple OEM meters
 - Water meter data can be integrated with any municipal water billing system through API's or file transfer methods
- e. Accessories available for turnkey offering
Available accessories include mounting kits, multiple antenna options depending on install requirement, as well as all necessary wire, crimps, and hardware.
- f. Thoroughness of the vetting process used to select partners
We do not use partners for this application. Should installs be required as part of a turnkey solution, third-party recommendations can be provided upon request.
- g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution
Full Factory Acceptance Test (FAT) completed and documented prior to shipment/deployment.

3 - Description of turnkey system planning, coordination and process:

Offers shall describe how they will address the following areas that shall be included in the turnkey package.

The description included in the proposal will be scored based on the suitability of the plan to government needs.

- a. Pre-installation coordination
Site Survey and Solution Discovery planning is completed by the assigned Project Manager through collaboration with the client. Site Survey Document is completed and fully documented based on project needs. Site Survey is provided to the customer for final acceptance and approval.
- b. Project coordination
LEC Project Management and Engineering Resources are assigned based on application/solution type and needs. Project management stays engaged throughout every stage of the process. Depending on project scope, reoccurring team calls are scheduled to meet project demands, timelines and expectations with Project Reports provided on a consistent basis.

c. Installation and Testing process

Pilots are a common process in order to optimize the solution requirements and deployment model. Pre-Install testing is completed through FAT testing at LEC facilities prior to shipment, installation, and deployment. Installation is typically customer driven due to simplicity of install or utilizing existing 3rd party municipal vendor. All installation instructions and wiring diagrams are provided with real-time support during field installation and final functional testing.

d. Client Infrastructure and support assessment process

LEC provides infrastructure and assessment through the site-survey and then finalized during the completion of the quality assessment process.

e. End user Acceptance process

- Completion of iQ Pulse Quality Assurance Process Document
- 30, 60, and 90 Day QA customer engagement process
- Solution Training/Refinement process
- SolveIT Support Tool training
- Final customer sign-off at 30-60-90 days depending on defined success criteria

f. Approach to maintenance and support

- 24/7/365 Access to SolveIT support ticketing system is standard
- Advanced notices of system maintenance and upgrades provided
- iQ Pulse Feature and Functionality upgrade notices provided
- Standard Support Services as provided in iQ Pulse Services Agreement
- Extended Support Services available
- See support process document attached

g. Initial and Ongoing Training provided

- iQ Pulse User and Admin Training prior to deployment
- 30, 60, and 90-day Training Program as part of the iQ Pulse Quality Assurance process
- Training for iQ Pulse feature additions provided upon request
- End user and Admin Video Training series available to all LEC Customers

h. On-going support and enhancement over the life of the agreement

See attached iQ Pulse services agreement.

4 - Service Factors:

a. Description of related services included in Turnkey Solution

LEC Turnkey Solutions include:

- Customer Site Survey Support
- IIoT Communications Hardware-From list of iQ2-Ready UL 508A Certified devices
- Delivery of all related wiring and installation diagrams
- Installation support
- Private Cellular Network Connectivity
- Site Engineering Support Admin and User Access to the iQ2 Remote Monitoring and Control Platform
- 24/7/364 Access to SolveIT Support Tool

- b. Experience and qualifications of partners and subcontractors
LEC does not utilize partners or subcontractors on a standard deployment.
- c. Description of Additional Integration and Consulting Services provided
- Site Survey Support Services
 - IIoT Engineering Support Services
 - Network Engineering Services
 - LEC Installation Services

See Attached "Product and Services Guide" for the full list of LEC Products and Services.

EXHIBIT D

SUPPLIER TERMS AND CONDITIONS

iQPulse™ TERMS AND CONDITIONS AGREEMENT

YOU MUST READ THIS iQPulse™ TERMS AND CONDITIONS AGREEMENT CAREFULLY. THE SERVICE IS PROVIDED TO THE CUSTOMER SUBJECT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT.

Section 1. Definitions.

1.1 "Agreement" means this iQPulse™ Terms and Conditions Agreement, as may be amended from time to time in accordance with the terms and conditions hereof.

1.2 "Communication Facility(ies)" means any wired or wireless instrumentality or service (or any combination thereof) used as a pathway for enabling Customer's use of the Service, including the Internet.

1.3 "Company" means LEC, Inc., a Mississippi business corporation, having its principal offices located at 110 Excell Drive Pearl, Mississippi 39208, together with each entity that it directly or indirectly owns or controls.

1.4 "Components" means the individual modules, features or products that make up the System. From time to time, new Components may be introduced, and access to those Components may be restricted depending on the terms of the particular Service.

1.5 "Connectivity Agreement" means the agreement between USCC and Customer governing Customer's subscription to any Communication Facility(ies) provided by USCC in connection with the Service.

1.6 "Customer" means the individual or entity who is a subscriber to any Communication Facility(ies) provided by USCC in connection with the Service.

1.7 "Customer Data" means any of Customer's information, documents, or electronic files that are either (A) transmitted through an Endpoint in connection with the Service, or (B) provided to Company hereunder for any purpose. At all times Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, security, appropriateness, ownership and permanent storage and safekeeping of all Customer Data.

1.8 "Effective Date" means the date of Customer's acceptance of this Agreement.

1.9 "Emergency System Maintenance" means any extraordinary, unscheduled maintenance to the System (or its Components) performed by Company for the purpose of immediately addressing any issue that affects the security or availability of the System.

1.10 "Endpoint(s)" means any iQPulse™ enabled device, or other device or asset generating Customer Data that is populated into the System.

1.11 "Event(s) of Default" means Customer's failure to perform or observe any other term, condition, or covenant to be performed by it under this Agreement.

1.12 "Force Majeure Event" means any (A) act(s) of war, hostility, or sabotage, including denial of service attacks; (B) act(s) of God; (C) electrical, Internet telecommunication outage or security breach that is not caused by the obligated Party; (D) government restrictions (including the denial or cancellation of any export or other license); and/or (E) any other event outside the reasonable control of the obligated Party.

1.13 "Notice" means any notice(s), consent(s), communication(s) and exchanges of information between the Parties as may be required hereunder. All Notices shall be provided in writing and shall be delivered personally, by registered or certified letter (return receipt requested), by courier or facsimile, and unless otherwise provided for in this Agreement shall be deemed effectively served (A) if by personal delivery, immediately upon such delivery; (B) if by registered or certified mail, five (5) calendar days after mailing; (C) if by courier, three (3) days after deposit; and (D) if by facsimile, immediately upon dispatch if receipt is confirmed electronically. All Notices shall be sent to the appropriate receiving Party's addresses as follows (or such other address as may have been furnished by or on behalf of such Party by like Notice): (i) if to Company – LEC, Inc., Post Office Box 127, Brandon, Mississippi 39043-0127; and (ii) if to Customer – the address identified as Customer's address in the Connectivity Agreement.

1.14 "Party" means Company or Customer, and every reference to a Party includes its successors and permitted assigns; and "Parties" means, collectively, Company and Customer and their respective successors and permitted assigns.

1.15 "Regular System Maintenance" means any regular, scheduled maintenance to the System (or its Components) performed by Company for the purpose of improving the functionality or security of the System.

1.16 "Service" means access to the System and its Components, together with certain additional related services, which depending upon the particular Service used by Customer may or may not include (A) temporary storage or backup of Customer Data; (B) hosting of Customer remote-site web pages(s); (C) remote troubleshooting (to the extent it relates to an embedded System device client application); (D) user-access management; (E) Customer support services; and (F) any other related services that Company may make available from time to time. Expressly excluded from the definition of Service are any and all Communication Facilities provided by Customer and/or any Third Party with whom Customer has an agreement to provide Communication Facilities.

1.17 "System" means the iQPulse™ platform, including any updates and improvements relating thereto and any derivative works of the foregoing. The System is made up of individual Components.

1.18 "Third Party" means any person or entity that is not a Party to this Agreement.

1.19 "USCC" means USCC Services, LLC, a Delaware limited liability company, having its principal offices located at 8410 W. Bryn Mawr, Chicago, Illinois 60631, together with each entity that its parent company United States Cellular Corporation directly or indirectly owns or controls. USCC is acting as a reseller of the Service.

Section 2. Rights and Restrictions of Use of the Service.

2.1 Customer Use Rights. During the Term hereof (as hereinafter defined) and subject to the terms and conditions of this Agreement, Company hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable right to connect the Endpoints to the Service for Customer's business purposes. The use right in the preceding sentence is strictly limited to the number of Endpoints as identified in the Connectivity Agreement. Said use rights are non-transferable, except in the event of a voluntary transfer of substantially all assets by Customer to a transferee which executes Company's form of agreement agreeing to be bound by all of the terms and conditions of this Agreement. All rights in and to the use of the Service not expressly granted to Customer herein are reserved to Company, and Customer agrees that Customer does not acquire any rights to use the Service in excess of the scope and/or duration of the term of this Agreement; provided, however, that Customer shall retain all ownership and intellectual property rights in and to the Customer Data. The rights of Customer to use the Service on a particular Endpoint cannot be shared or used by, on or for more than one Endpoint. To the extent that it may be appropriate or necessary in any particular Customer application to utilize any Third Party hardware,

software or technology with the Service, Customer's right to use such Third Party hardware, software or technology shall be governed by the terms of the applicable Third Party hardware, software or technology license agreement and not under this Agreement. To the extent that the Service may enable Customer to add links to web sites and access to content, products and services of any third parties (including users, advertisers, affiliates and sponsors of such third parties), Company is not responsible for any such Third Party web sites or Third Party content provided on or through the Service and Customer assumes and shall bear any and all risks associated with the access and use of such web sites and Third Party content, products and services. Upon the expiration or earlier termination of this Agreement as provided herein, all rights of Customer to use the Service shall terminate.

2.2 Availability of Service. At all times during the Term hereof, Company warrants that Company will provide to Customer access to the Service on a twenty-four (24) hours, seven (7) days per week basis at an availability rate of at least ninety-nine point nine percent (99.9%) (the "Service Uptime"). Service Uptime shall be calculated to the nearest minute occurring during each calendar month of the Term and shall be continuously monitored through Company's automated systems.

2.3 System Maintenance. Company may perform Regular System Maintenance on an as-needed basis (typically occurring between the hours of 9:00 P.M. and 4:00 A.M. Pacific Time), which in certain circumstances may result in an interruption of Service Uptime. Company will provide to Customer a minimum of fifteen (15) days advance Notice of any Regular System Maintenance to be conducted, and in circumstances where an interruption in Service Uptime is expected to occur shall specify in said Notice the anticipated duration of such interruption. In unexpected circumstances where Company is required to perform Emergency System Maintenance, Company will provide to Customer advance Notice of any Emergency System Maintenance as reasonably possible under the circumstances.

2.4 Storage and Backup of Customer Data. In the event that the Service subscribed to by Customer includes the temporary storage or backup of Customer Data (as applicable), Company will temporarily store or backup any Customer Data populated to the System (or portion thereof as may be designated by Customer) up to a maximum of either (A) a period of twelve (12) months, or (B) a limit of five hundred thousand (500,000) database records, whichever occurs first; provided, however, that the foregoing database record limit may be affected by the configuration of the device(s) comprising each Endpoint and/or the specific data value update rates determined by Customer's use of the Service.

2.5 Customer Support. Company agrees to provide normal Customer support on weekdays between the hours of 8:00 A.M. and 5:00 P.M. Central Time, during which time Company will respond to a request for Customer support within one (1) hour or less. Further, Company agrees to provide after-hours Customer support on weekdays between the hours of 5:00 P.M. and 8:00 A.M. Central Time and on weekends via Company's solveIT® ticketing system, during which time Company will respond to a request for Customer support no later than 10:00 A.M. Eastern Time the following business day.

2.6 Company Use Rights. During the Term and subject to the terms and conditions of this Agreement, Customer hereby grants to Company a non-exclusive, non-transferable, non-sublicensable right to use, copy, transmit, store, modify and display the Customer Data solely for purposes of Customer's use of the Service; otherwise, Company shall not use the Customer Data except to improve the Service and/or as necessary to perform its obligations hereunder. Company may compile statistical information related to the performance of the Service, and at its election make such information publicly available, provided that such information does not incorporate Customer's identify, any Customer Data, and/or any of Customer's Confidential Information (as hereinafter defined), and Company shall retain all intellectual property rights in and to such information.

2.7 Customer Use Restrictions. At all times during the Term hereof, Customer expressly covenants and agrees not to use or permit use of the Service, including without limitation by uploading, emailing, posting, publishing or otherwise transmitting any Customer Data or other material, for any purpose that may (A) menace or harass any person or cause damage or injury to any person or property; (B) involve

the publication of any material that is false, defamatory, harassing or obscene; (C) violate privacy rights or promote bigotry, racism, hatred or harm; (D) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (E) constitute an infringement of intellectual property or other proprietary rights of any Third Party; or (F) otherwise violate applicable laws, ordinances or regulations. In addition to any other rights afforded to Company hereunder, Company expressly reserves the right to suspend access to the Service for any violation of the foregoing restrictions and shall have no liability to Customer in the event that such action is taken. Customer expressly acknowledges that the Service is not intended for use with protected health information under HIPAA, credit card numbers, financial account numbers, or other similarly-sensitive personal information, and that Customer assumes all risk arising from use of any such sensitive information with the Service, including the risk of any inadvertent disclosure or unauthorized access thereto. Customer is responsible for ensuring that Customer's use of the Service is in compliance with all applicable laws and governmental regulations (including without limitation those set forth in Section 7 of this Agreement), and Customer acknowledges that Customer assumes all risk arising from any such use that is not compliant with applicable laws and regulations.

2.8 Other Restrictions. In addition to those restrictions set forth in Section 2 hereof, with respect to either the Service and/or the System, as applicable, Customer shall not, directly, indirectly, alone, or with another party either (A) remove or modify any Company markings or any statement or declaration of Company's proprietary rights; copy, disassemble, reverse engineer, or decompile the System; (B) modify, create derivative works based upon, or translate the System; (C) license, sell, rent, lease, transfer, grant any rights in or otherwise commercially exploit the Service in any form to any other party; (D) access or use the Service in order to build or support, and/or assist a Third Party in building or supporting, products or services competitive to Company; (E) other than the Customer Data, disclose the results of the Service without Company's prior written consent; or (F) attempt to do any of the foregoing or cause or permit any Third Party to do or attempt to do any of the foregoing. At all times Company shall own all right, title and interest in and to any and all intellectual property rights (including all derivatives or improvements thereof) in the Service, and any suggestions, enhancement requests, feedback, recommendations or other information provided by Customer relating to the Service.

3. Non-Disclosure of Confidential Information. By virtue of this Agreement, the Parties may have access to one-another's information that the owning Party considers confidential in nature (the "Confidential Information"). Accordingly, each Party expressly covenants and agrees to disclose only information that is required for the performance of their respective obligations under this Agreement. The term "Confidential Information" shall also include the terms under this Agreement, any Customer Data residing in the System environment, and all information clearly identified as confidential at the time of its disclosure. However, a Party's Confidential Information shall not include information that: (A) is or becomes a part of the public domain through no act or omission of the other Party; (B) was in the other Party's lawful possession prior to the disclosure and had not been obtained by the other Party either directly or indirectly from the disclosing Party; (C) is lawfully disclosed to the other Party by a Third Party without restriction on the disclosure; or (D) is independently developed by the other Party. Each Party agrees to hold one another's Confidential Information in confidence for a period of three (3) years subsequent to the expiration or termination of this Agreement, and further agrees to disclose Confidential Information only to its employees or agents who are required to protect it against unauthorized disclosure in a manner no less protective than under this Agreement, and in any event only for the purpose of performing a Party's obligations hereunder. Nothing shall prevent either Party from disclosing the terms under this Agreement in any legal proceeding arising from or in connection with this Agreement or from disclosing the Confidential Information to a governmental entity as may be required by applicable law.

Section 4. Term and Termination.

4.1 Term. The term of this Agreement (the "Term") commences on the Effective Date and remains in effect for the duration of the term of the Connectivity Agreement. The Term will automatically terminate upon the termination or expiration of the Connectivity Agreement. For a period of up to thirty (30)

days subsequent to the effective date of the expiration or termination of this Agreement, upon receipt of written request Company may permit Customer to access the Service solely to the extent necessary for Customer to retrieve any Customer Data to the extent that any such Customer Data resides in the System environment; provided, however, that Customer expressly acknowledges and agrees that Company has no obligation to retain any Customer Data and that any Customer Data residing in the System environment may be irretrievably deleted at any time after thirty (30) days subsequent to the expiration or termination of this Agreement.

4.2 Termination of Service. The Service may be terminated by Company upon the occurrence of an Event of Default by Customer if such Event of Default is not cured by Customer within thirty (30) days subsequent to receipt of a Notice of the Event of Default; provided, however, that in any case of any violation by Customer of Section 2 of this Agreement, the Service may be terminated immediately by the Company.

Section 5. Warranty Disclaimer and Liability.

5.1 Warranty Disclaimer. AS COMPANY DOES NOT CONTROL THE TRANSFER OF DATA OVER OR THROUGH ANY COMMUNICATION FACILITIES, CUSTOMER EXPRESSLY ACKNOWLEDGES AND AGREES THAT (A) COMPANY DOES NOT GUARANTEE THAT THE SERVICE WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT COMPANY WILL BE ABLE TO CORRECT ALL SERVICE ERRORS; (B) THE SERVICE MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATION FACILITIES; AND (C) COMPANY IS NOT RESPONSIBLE FOR ANY ERRORS, DELAYS, DELIVERY FAILURES, OR OTHER DAMAGES THAT MAY RESULTING FROM SUCH PROBLEMS. TO THE EXTENT NOT PROHIBITED BY LAW, EXCEPT AS OTHERWISE PROVIDED HEREIN THERE ARE NO EXPRESS OR IMPLIED WARRANTIES FOR OR CONDITIONS TO THE SERVICE HEREUNDER, INCLUDING COMPATIBILITY OF THE SERVICE WITH ANY SPECIFIC HARDWARE, SYSTEMS, COMMUNICATION FACILITIES, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

5.2 Liability Disclaimer. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF ANY CUSTOMER DATA, REVENUE OR PROFITS (EXCLUDING FEES PAYABLE BY CUSTOMER TO COMPANY UNDER THIS AGREEMENT). COMPANY'S MAXIMUM LIABILITY TO CUSTOMER FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNTS ACTUALLY PAID BY CUSTOMER TO USCC (AS RESELLER) FOR THE SERVICE THAT IS THE SUBJECT OF THE CLAIM IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM

6. Indemnification. In the event that any Third Party should make a claim against either Customer or Company (the "Recipient," which may refer to either Customer or Company depending upon which Party receives the Material), that any information, design, specification, instruction, software, service, data, or material (collectively the "Material") furnished by either Customer or Company (the "Provider," which may refer to either Customer or Company depending on which Party provides the Material), and used by the Recipient infringes on such Third Party's intellectual property rights, the Provider, at its sole cost and expense, shall defend the Recipient against the claim and indemnify the Recipient from any damages, liabilities, costs and expenses awarded by a court of competent to the Third Party claiming infringement or the settlement agreed to by the Provider, provided that the Recipient does all of the following: (A) promptly notifies the Provider in writing, but in no event later than thirty (30) days subsequent to when the Recipient receives Notice of the claim (or sooner if required by applicable law); (B) gives the Provider sole control of the defense and any settlement negotiations; and (C) gives the Provider the information, authority, and assistance the Provider needs to defend against or settle the claim. In the event the Provider believes or it is determined that any of the Material may have violated a Third Party's intellectual property rights, the

Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for its continued use, or in the event that these alternatives are not commercially reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such return materially affects Company's ability to meet its obligations hereunder, then Company may, at its option and upon providing thirty (30) days prior written Notice to Customer, terminate this Agreement. The Provider will not indemnify the Recipient if the Recipient alters the Material or uses it outside the scope of use identified in the Provider's user documentation or services policies or if the Recipient uses a version of the Materials which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was provided to the Recipient. The Provider will not indemnify the Recipient to the extent that an infringement claim is based upon (i) any information, design, specification, instruction, software, data, or material not furnished by the Provider, or (ii) any Material from a Third Party portal or other external source that is accessible to Customer within or from the Service (e.g., a Third Party web page accessed via a hyperlink). Notwithstanding any of the foregoing, Company has no obligation to indemnify Customer in any circumstance where (a) any infringement claim is based upon the combination of any Material with any products or services not provided by Company; (b) any infringement is caused by the actions of Customer against any Third Party if the Service as delivered to Customer and used in accordance with the terms of this Agreement would not otherwise infringe any Third Party intellectual property rights; or (c) any infringement claim is based on (1) a patent that Customer was made aware of prior to the Effective Date of this Agreement (pursuant to a claim, demand, or Notice), or (2) any of Customer's actions occurring prior to the Effective Date of this Agreement. It is the express intent of the Parties that this Section 6 provides each Party's exclusive remedy for any infringement claims or damages.

7. Compliance with Export Laws. The export laws and regulations of the United States as well as other relevant local export laws and regulations may apply to the Service. Customer expressly acknowledges and agrees that (A) to the extent applicable, such export control laws may govern Customer's use of the Service under this Agreement; (B) Customer shall comply with all such applicable export laws and regulations; (C) no data, information, software programs and/or materials resulting from Service (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

8. Force Majeure. Neither Party shall be responsible for any failure or delay in the performance of their respective obligations hereunder provided such failure or delay is caused by a Force Majeure Event; provided, however, that each Party expressly covenants and agrees to use reasonable efforts to mitigate the effect of a Force Majeure Event that should occur during the Term of this Agreement. In the event that a Force Majeure Event occurs and continues for more than thirty (30) days, either Party may cancel any unperformed service upon providing advance written Notice to the other Party.

9. Other Provisions. Time is of the essence of each of the provisions of this Agreement. Customer shall not assign, transfer or encumber this Agreement without obtaining prior written consent of Company, nor shall any attempted assignment, transfer or encumbrance of this Agreement be effectuated by operation of law or otherwise without the prior written consent of Company. Company may assign or transfer this Agreement to any affiliate without obtaining consent from Customer, written or otherwise, and such assignment or transfer shall be effective immediately upon execution and delivery by Company. The Parties hereto expressly acknowledge and agree that, as between the Parties, (A) except as otherwise expressly set forth herein, no representation(s) has been made with respect to the subject matter of this Agreement, nor any representations inducing the execution and delivery of this Agreement; (B) each Party has relied on such Party's own judgment in entering into this Agreement; and (C) any statements and/or representations that may have been made previously by either of them to the other are void and of no effect, and that neither of them has relied upon such statements and/or representations in connection with such Party's dealings with the other. The Parties expressly agree that it is their intention and covenant that

(i) this Agreement constitutes the entire agreement between the Parties regarding the subject matter hereof, and that any and all prior agreements, proposals or communications (whether oral or written) between the Parties are superseded by and merged into this Agreement; (ii) this Agreement, any performance under this Agreement, and all suits and proceedings arising out of, related to, in connection with or by reason of this Agreement between the Parties, be construed in accordance with, and under and pursuant to, the laws of the State of Mississippi; (iii) the laws of the State of Mississippi will be applicable and will govern any action or other proceeding that may be brought by either Party arising out of, related to, in connection with or by reason of this Agreement, to the exclusion of the law of any other forum; (iv) unless expressly waived by Company, the exclusive jurisdiction and venue of any legal action between the Parties with respect to the subject matter of this Agreement shall be the appropriate court(s) in the Southern District of Mississippi; and (v) each of the Parties hereto submits itself to the exclusive jurisdiction and venue of such court(s) for the purpose of any such legal action. If it becomes necessary for any Party to undertake any litigation or to employ an attorney to assist such Party in pursuit of or protection of its rights under this Agreement, the non-prevailing Party shall be obligated to reimburse the prevailing Party for such fees and related costs and expenses, including reasonable attorney's fees, whether incurred at trial, on appeal, or otherwise. The invalidity, illegality, or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if such invalid, illegal, or unenforceable provision had been omitted. This Agreement may be modified or amended by Company from time to time, and where material modifications or amendments are made Company will provide appropriate notice to Customer in such circumstances, whereupon Customer's continued use of the Service will constitute and express acceptance of such modifications or amendments. All terms and conditions of this Agreement shall be binding upon the successors and assigns of the Parties hereto. No waiver of any provision of this Agreement shall be implied by any failure of either Party to enforce any remedy upon the violation of such provision, even if such violation is continued or repeated subsequently. No express waiver shall affect any provision other than the one specified in such waiver, and that only for the time and in the manner specifically stated. Captions to and headings of the Sections and paragraphs of this Agreement are solely for the convenience of the Parties and shall not be used for the interpretation or determination of the validity of the Agreement and/or any provision(s) hereof. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine, neuter, singular or plural as the identity of the person or persons may require. Provisions that survive expiration or termination of this Agreement are those provisions relating to limitation of liability, infringement indemnity and any others which by their nature are intended to survive.

4820-4721-4247, v. 1



iQ2® / iQCommSentry®
WIRELESS SERVICE AGREEMENT No. _____

EXHIBIT "A" (V1) xx/xx/20xx

Business Name
Address
City State Zip
Telephone
Email

Effective Date:

Agreement Term:

Node Summary:

Site	Information

Monthly Charges:

Description	Quantity	Unit Price	Extension

SPECIAL PROVISIONS:

iQ2® / iQCommSentry® WIRELESS SERVICE AGREEMENT

THIS iQ2® / iQCommSentry® WIRELESS SERVICE AGREEMENT (the "Agreement") is made and entered into by and between LEC, INC., a Mississippi Business Corporation (the "Company") and _____, (the "Customer"). Company and Customer may hereinafter be referred to as a "Party" in the singular and the "Parties" collectively.

Section 1. Definitions.

1.1 "Affiliate" of a Party means any entity that controls, is controlled by, or is under common control with, such Party.

1.2 "Acceptable Application" means a software program, application or platform that will be combined with the Service and used by Customer or end users and which is compatible with the efficient operation of the Network, does not interfere with the services of other parties, does not result in inefficient or excessive use of the Network or the networks of Company's roaming carriers, and is not inconsistent with Network policies and practices.

1.3 "Approved Device" means a Device that has been certified and approved by Company.

1.4 "Area(s)" means the areas within the United States where Company is licensed to provide the Service and is providing Service. The Area may change from time to time.

1.5 "Device" means the equipment used by a Customer to originate or receive wireless transmissions on the Network, including any machine to machine communications unit, wireless modem, SIM, and any accessories. Cellular telephone(s) are expressly excluded from this definition.

1.6 "Equipment" means all equipment (other than equipment comprising portions of the Network) necessary to enable Customer to use or benefit from the Service, including but not limited to Customer's network facilities and any Device.

1.7 "Events of Default" means the following: (i) the execution of any assignment for the benefit of creditors or the filing for relief by either Party under any applicable bankruptcy, reorganization, moratorium, or similar debtor relief; (ii) the appointment of a receiver for Customer or Company or for substantially all of their respective assets or properties; (iii) Customer's failure to pay any sum owed to the other hereunder at the time such amount comes due; (iv) either Party's failure to perform or observe any other term, condition, or covenant to be performed by it under this Agreement; (v) an unauthorized assignment of this Agreement; or (vi) Customer's failure to utilize Equipment compatible with the Network or other network of Company, as determined by Company.

1.8 "Hosting Services" means access to the iQ2® / iQCommSentry® interface (as applicable), together with certain additional related services which may include private cellular network access, periodic firmware upgrades to the Service Devices (when necessary), temporary storage of Customer data, hosting of Customer remote-site web pages(s) (when applicable), remote troubleshooting, user-access management, carrier support and twenty-four (24) hour customer service. In certain cases, Hosting Services may also include custom Virtual Private Network configuration and maintenance, content filtering, usage monitoring and limiting, data pooling, network architecture and configuration assistance, transmission of data log(s) to Customer, site-to-site communication and alarm messaging.

1.9 "Machine to Machine Communications" means wireless communications made possible by the provisioning of an Approved Device or the insertion of a SIM by Customer or its agent into an Approved Device (as applicable) for use with an Acceptable Application upon activation of the Service, for use by Customer.

1.10 "Network" means those integrated mobile switching facilities, servers, cell sites, connections, billing systems and other related facilities used by Company to provide Service in an Area.

1.11 "Service" means the Hosting Services, and any machine to machine data and SMS wireless telecommunications services (as and where available) for GSM communications, GPRS (General Packet Radio Services), EDGE, Universal Mobile Telephone Service (UMTS), High Speed Packet Access (HSPA) Service, High Speed Packet

Access + (HSPA+), Code Division Multiple Access Service (CDMA), Enhanced Voice-Data Optimized Service (EVDO) or Long Term Evolution (LTE) technology. Service does not include any voice service.

1.12 "Service Plan" means the particular set of rates, terms and conditions as stated in the Exhibits to this Agreement upon which Company makes Service available to Customer, but does not include any short-term marketing promotions that may periodically be offered by Company.

1.13 "Subscriber Identity Module ("SIM")" means a specially programmed microchip that is inserted into a Device which encrypts transmissions and identifies the user to the Network.

1.14 "Subscription Fraud" means using or assisting another to use any scheme, false representation, or false credit device, or other fraudulent means or devices in connection with Service or any Service Device.

1.15 "Unauthorized Access" means any unauthorized use of the Service or any Service Device, which includes the practices generally referred to as "counterfeiting," "cloning fraud," or "tumbling fraud."

TERMS AND CONDITIONS

Section 2. Purchase and Sale of the Service. Customer agrees to purchase from Company, and Company agrees to sell to Customer, the Service for use in Machine to Machine Communications on Company's wireless Network as stated in the Exhibits hereto. The Service is provided to Customer for Customer's use and not for resale. The Service (other than roaming service) is only available in the Area. At all times Customer will comply with Company policies and procedures reasonably established by Company for providing the Service, and Company may from time to time modify these policies and procedures.

Section 3. Term. This Agreement commences on the Effective Date and remains in effect for the length of the Agreement Period as both are identified in Exhibit A attached hereto and incorporated herein by reference (the "Term"). This Agreement will automatically renew for successive one (1) year renewal Term(s) unless either Party provides the other with a notice of termination at least thirty (30) days prior to the end of the then-current Term.

Section 4. The Service.

4.1 Network Connections. Customer must connect to the Network in order to receive the Service. Such connections may be obtained under this Agreement or pursuant to separate agreement between the Parties.

4.2 General Service Requirements. Company will only activate Service for use with the Acceptable Applications and Approved Device(s). Company may require a minimum number of Device(s) to be activated at one time. To the extent that SIMs are required for Service, Customer is only authorized to purchase SIMs directly from Company or through Company's Affiliate(s) for use on the Network. Unless otherwise stated, an Approved Device, an Acceptable Application(s) and a SIM (when applicable) are required for all Service Plans. Company may, at its option, require Customer to provide information about how their applications interact with the Network, and may limit, restrict or prohibit use of applications in Company's sole discretion.

4.3 Service Requiring Use of SIMs. A number may not be associated with more than one SIM at the same time, unless otherwise approved by Company. Company may deny Service to any SIM(s) without liability to Customer for SIMs appearing on Company's service deny lists for reasons including, but not limited to, cases where the SIM is stolen, has been used for fraudulent purposes, is not used in an Approved Device or with an Acceptable Application, or is defective, and Company will notify Customer in such cases. Customer must not insert any SIM into anything other than an Approved Device, and/or program, re-program or tamper with any SIM in any manner, and Customer shall be responsible for the payment of any and all charges incurred resulting from any violation of this Agreement.

4.4 Modification or Termination of Service. If Customer desires to modify or terminate any Service or change Service Plans, Customer must advise Company in writing accordingly. Changes will become effective as determined by Company. Should Customer terminate Service under this Agreement at any time during the Term (or any renewal thereof as provided in Section 3), Customer shall pay to Company an early termination fee in an amount equal to fifty percent (50%) of the total balance of the Service Plan for the remaining current Term.

4.5 Troubleshooting. Customer will cooperate with Company in any troubleshooting of the Equipment or the Network as required to maintain the efficient operation of the Service.

4.6 Limitations on Roaming Service.

4.6.1 THE AVAILABILITY OF ROAMING SERVICES, AND THE CHARGES FOR THOSE SERVICES, IS DEPENDENT IN PART ON THE TYPE OF EQUIPMENT USED BY CUSTOMER AND THE PROGRAMMING OF THAT EQUIPMENT. COMPANY MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE AVAILABILITY OR QUALITY OF ROAMING SERVICE PROVIDED BY OTHER WIRELESS NETWORKS, AND COMPANY WILL NOT BE LIABLE IN ANY CAPACITY FOR ANY ERRORS, OUTAGES, OR FAILURES OF ROAMING SERVICES PROVIDED BY OTHER WIRELESS NETWORKS.

4.6.2 IF COMPANY, OR ANOTHER ENTITY WITH WHOM COMPANY HAS A ROAMING AGREEMENT, DISCOVERS OR SUSPECTS ABUSE OR FRAUD WITH RESPECT TO CERTAIN NUMBERS, THEN ROAMING PRIVILEGES MAY BE SUSPENDED WITH RESPECT TO SUCH NUMBERS. COMPANY WILL USE COMMERCIALY REASONABLE EFFORTS TO PROVIDE CUSTOMER WITH PRIOR, OR PROMPT SUBSEQUENT, NOTIFICATION OF THE SUSPENSION OF THE ROAMING SERVICE. COMPANY WILL NOT BE LIABLE IN ANY CAPACITY TO CUSTOMER FOR THE UNAVAILABILITY OR SUSPENSION OF ROAMING SERVICE BY OTHER CARRIERS.

4.6.3 TO THE EXTENT ACCESS TO ROAMING CAPABILITIES IS PROVIDED BY COMPANY TO CUSTOMER, IT IS DEEMED TO BE A "SERVICE" AS DEFINED IN SECTION 1, AND THE USE OF SUCH ROAMING BY CUSTOMER WILL BE GOVERNED BY THE PROVISIONS OF THIS AGREEMENT.

4.7 Service Technology Disclosures. The underlying carrier is not obligated to maintain any particular technology, and Network technologies may be terminated at any time in its sole discretion. Company will provide Customer twelve (12) months prior written notice of any termination of a significant wireless technology on a nationwide basis.

4.8 International Roaming. Service is not permitted to be used under this Agreement for international roaming, except on a rare and incidental basis. Should Company, in its sole discretion, determine that Customer is utilizing international roaming more frequently than on a rare and incidental basis, Company may terminate such international roaming with or without notice to Customer of such termination. With respect to any international roaming under this Agreement, Customer (i) shall provide Company with all assistance reasonably required to enable Company to comply with requests or requirements of a roaming carrier, regulator, or other governmental body relating to Customer's use of international roaming; (ii) shall comply with each country's legal and regulatory requirements arising from or relating to Customer's use of the Service; (iii) shall provide Company with the place of primary use of the Service (which must be its business street address and be within an eligible Company wireless Service area); (iv) expressly acknowledges that Service may not be available outside of a provisioned roaming zone; and (v) shall indemnify and hold Company harmless from any claims, costs, losses or damages resulting from Customer's international roaming.

4.9 PRIVACY. THE NETWORK HAS MANY COMPLEX ELEMENTS AND IS NOT GUARANTEED AGAINST EAVESDROPPERS, HACKERS, DENIAL OF SERVICE ATTACKS, VIRUSES, OR INTERCEPTORS. CUSTOMER AGREES THAT COMPANY WILL NOT BE LIABLE TO CUSTOMER OR TO END USERS FOR ANY LACK OF PRIVACY OR SECURITY. IN THE EVENT THAT CUSTOMER SUBSCRIBES TO AN UNMANAGED SERVICES PLAN, CUSTOMER EXPRESLY ACKNOWLEDGES AND AGREES THAT CUSTOMER SHALL BE SOLELY REPONSIBLE FOR ANY AND ALL SECURITY AND DATA MONITORING ASSOCIATED WITH SUCH SERVICE PLAN.

Section 5. DISCLOSURE AND ACKNOWLEDGMENT. CUSTOMER UNDERSTANDS AND AGREES (I) THAT CUSTOMER HAS NO CONTRACTUAL RELATIONSHIP WITH THE UNDERLYING WIRELESS SERVICE CARRIER/PROVIDER; (II) THAT CUSTOMER IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN COMPANY AND THE UNDERLYING CARRIER/PROVIDER; (III) THAT THE UNDERLYING CARRIER/PROVIDER HAS NO LEGAL OR EQUITABLE LIABILITY OF ANY KIND TO CUSTOMER WHATSOEVER, WHETHER FOR BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE, AND CUSTOMER HEREBY WAIVES ANY AND ALL CLAIMS OR DEMANDS THEREFORE; (IV) THAT MESSAGES MAY BE DELAYED, DELETED OR NOT DELIVERED; AND (V) THAT THE UNDERLYING CARRIER CANNOT GUARANTEE THE SECURITY OF WIRELESS TRANSMISSIONS AND WILL NOT BE LIABLE FOR ANY LACK OF SECURITY RELATING TO THE USE OF THE SERVICES.

Section 6. Rates.

6.1 Service Plans. Customer will pay for Service at the rates set forth in the applicable Service Plan(s) as selected by Customer. Rate plan changes will take effect as stated in the Exhibits. Company may modify a Service Plan or charge at any time by providing thirty (30) days advance written notice to Customer, provided that any modification not adverse to Customer may be made immediately effective upon written notice.

6.2 Service Outages. In the event of a total Service outage within an Area which is not caused by Customer and which lasts for a period of twenty-four (24) hours or more, a credit allowance will be made at Customer's request in the form of a pro rata adjustment of the fixed charges billed by Company to Customer with respect to the affected SIM(s). Periods of discontinuous outage may not be accumulated in determining if an outage has continued for at least twenty-four (24) hours. In order to receive such credit, Customer must submit a written request to Company, stating the date and location of the outage, the SIMs affected, and such other information as Company may reasonably require. Such notice must be received by Company within ten (10) business days following the last date of the period of outage. EXCEPT AS PROVIDED HEREIN, COMPANY WILL NOT INCUR ANY LIABILITY OF ANY NATURE OR TYPE WHATSOEVER FOR SERVICE OUTAGES.

Section 7. Invoices, Payments, Disputed Charges and Billing Data.

7.1 Invoices and Billing Data. Company will provide Customer a summary invoice for all charges on a monthly basis, normally within ten (10) days subsequent to the cut-off date for each billing cycle, each such invoice containing all charges and applicable taxes and/or regulatory fees. All SIMs will be placed on the same billing cycle. Customer must notify Company if Customer has not received an invoice within twenty (20) days subsequent to the bill cycle cut-off date. Company will use reasonable efforts to provide electronic detailed billing data for all Service Plans loaded into a billing cycle.

7.2 Payments. Payment in full for each invoice is due at the location set forth in the invoice, in a form payable in U.S. currency, upon the due date set forth in the invoice or within thirty (30) days subsequent to receipt of the billing data (which shall include any amounts due for data usage in excess of the allotted amount for the then-current billing period), whichever is later (the "Due Date"). For purposes of payment, Customer may rely only on the invoice and other billing data received from Company, and may not rely on any other source including information drawn from any Company or Customer system. Depending on Customer's payment history, Company may at its sole discretion require payment by certified check, money order, or wire transfer. Payments are past due, and Customer will have committed an Event of Default, if not received by the Due Date. Time is of the essence with respect to payment of Company's invoices. If a payment becomes past due, the account will accrue late fees and interest at the rate of one and one-half percent (1.50%) per month or the maximum lawful rate, whichever is greater. Customer agrees not to place any condition or restrictive legend, such as "Paid in Full", on any check or financial instrument used to make a payment. The Parties agree that the negotiation of any such check or instrument so inscribed will not constitute an accord and satisfaction or novation.

7.2.1 Suspension of Service. In the event that Customer fails to timely make payments to Company as required in this Agreement, Company may suspend the Service at any time. During the pendency of any suspension of Service, all charges, fees and taxes for Service will continue to accrue, and Customer will continue to be financially responsible for the payment of such amounts. In order to restore any suspended Service, Customer shall pay a reactivation fee in the additional amount of One Hundred United States Dollars (\$100.00) per Device.

7.3 Disputed Charges. If Customer disputes part of the monthly invoice, Customer is required to notify Company in writing and to submit appropriate documentation justifying such dispute to Company as soon as it is aware of the dispute, but in no event later than the thirty (30) days after the invoice Due Date or such dispute is waived. Notwithstanding any such dispute, Customer agrees to pay the full amount of any such bill pending the resolution of such dispute. Company will respond to Customer's written dispute within thirty (30) days of receipt of such dispute. Company and Customer agree to use best efforts to resolve all disputes and Company agrees to promptly refund any amounts due upon dispute resolution. The notice requirements in this Paragraph 7.3 will not shorten the period within which actions must be filed as established by the applicable statute of limitations, but will constitute a condition precedent to any right of the aggrieved Party to contest prior invoices or payments. This condition is designed to allow each Party the opportunity to preserve important evidence in defense of a claim.

Section 8. Abusive or Fraudulent Use.

8.1 Generally. Service may be restricted or cancelled if there is a reasonable suspicion of abuse or fraudulent use. Company will provide prompt notice of the restriction or termination to Customer. Customer agrees to make good faith efforts to minimize abuse or fraudulent use, to promptly report to Company any such abuse or fraudulent

use of which Customer becomes aware, and to cooperate in any investigation or prosecution initiated by Company. Customer also agrees that Company may in its discretion disable any Device, or otherwise block access to the Service when suspected of abuse or fraudulent use. Abuse and fraudulent use of Service include, but are not limited to (i) attempting or assisting another to access, alter, or interfere with the communications of and/or information about another wireless customer; (ii) tampering with or making an unauthorized connection to the Network; (iii) installing any amplifiers, enhancers, repeaters, or other devices that modify the radio frequencies used to provide the Service; (iv) Subscription Fraud; (v) using Service in such a manner so as to interfere unreasonably with the use of Service by one or more other wireless customers or to interfere unreasonably with Company's ability to provide Service; (vi) using Service to convey obscene, salacious, or unlawful information; (vii) using Service without permission on a stolen or lost Device; (viii) Unauthorized Access; (ix) using the Service to provide voice over IP services; and/or (x) extensive use of the Service outside of the Area.

8.2 Liability for Abuse or Fraudulent Usage. Customer is solely liable for charges, costs and damages resulting from (i) Subscription Fraud, (ii) any theft of a Device, any user identification number, or password associated with the Service; (iii) any abuse or fraud facilitated by Customer, Customer's employees, or Customer's agents, and/or (iv) any failure to give prompt notice of suspected abuse or fraudulent use based on information available to Customer.

Section 9. Limitation of Liability.

9.1 Generally. COMPANY'S ENTIRE LIABILITY, AND CUSTOMER'S EXCLUSIVE REMEDY, FOR DAMAGES ARISING OUT OF MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, LOSS OR CORRUPTION OF CUSTOMER'S DATA, ERRORS OR DEFECTS IN THE SERVICE(S), SHALL IN NO EVENT EXCEED THE SPECIFIED CREDITS UNDER THIS AGREEMENT, OR IF NO CREDITS ARE SPECIFIED, AN AMOUNT EQUIVALENT TO THE PROPORTIONATE CHARGE TO CUSTOMER FOR THE PERIOD OF SERVICE DURING WHICH SUCH MISTAKE, OMISSION, INTERRUPTION, DELAY, ERROR OR DEFECT IN THE SERVICES OCCURS AND CONTINUES. IN NO EVENT SHALL ANY OTHER LIABILITY ATTACH TO COMPANY.

9.2 Consequential Damages. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES, OR INCREASED COST OF OPERATIONS.

Section 10. Default and Termination.

10.1 Default. This Agreement may be terminated upon an Event of Default by either Party if such Event of Default is not cured by the defaulting Party within thirty (30) days subsequent to receipt of a notice of the Default; provided, however, that in the case of failure to pay invoices or in the case of a violation of Section 8 of this Agreement, this Agreement may be terminated if such Event of Default is not cured within ten (10) days subsequent to receipt of notice of the Event of Default.

10.2 Termination for Convenience. Company may terminate this Agreement at its convenience upon ninety (90) days' prior written notice to Customer.

Section 11. Installation Services Warranty. The Installation Services Warranty applies to all work performed by Company in connection with the establishment of the Service (the "Installation Services"). Company warrants and represents that the Installation Services shall be free from any material defect for a period of one (1) year subsequent to the commencement of the initial Term of this Agreement (the "Installation Services Warranty Period"). In the event that Customer notifies Company during the Installation Services Warranty Period that a defect in the Installation Services exists, Company agrees to provide such services as are reasonably necessary to correct said defect in the Installation Services at no cost to Customer; provided, however, that in the event Company in good faith determines that the alleged defect is not due to any fault of Company, or if Customer's notice is tendered subsequent to the expiration of the Installation Services Warranty Period, then Customer shall pay Company for all services provided to Customer in accordance with Company's then-current rate schedule. The Installation Services Warranty only applies to defects in the Installation Services and not defects in any Device(s) or Equipment, or defects caused by other circumstances, including without limitation accident, misuse, unforeseeable use, neglect, alteration, vandalism, improper installation by others, improper testing, improper repair and/or Acts of God.

Section 12. Other Provisions. All notices and other communications under this Agreement shall be in writing and shall be deemed given when delivered personally, transmitted by facsimile (provided that a copy of such facsimile is sent by certified mail, return receipt requested) or sent by certified mail, return receipt requested, to the Parties

address(es) of record. Time is of the essence of each of the provisions of this Agreement. Customer shall not assign, transfer or encumber this Agreement without obtaining prior written consent of Company, nor shall any attempted assignment, transfer or encumbrance of this Agreement be effectuated by operation of law or otherwise without the prior written consent of Company. Company may assign or transfer this Agreement to any Affiliate without obtaining consent from Customer, written or otherwise, and such assignment or transfer shall be effective immediately upon execution and delivery by Company. The person executing this Agreement on behalf of Customer expressly warrants and represents that he/she is the authorized representative of Customer and possesses the requisite authority to legally bind Customer to the terms and conditions hereof. The Parties hereto expressly acknowledge and agree that (i) except as otherwise expressly set forth herein, no representation(s) has been made with respect to the subject matter of this Agreement, nor any representations inducing the execution and delivery of this Agreement, (ii) each Party has relied on such Party's own judgment in entering into this Agreement, and (iii) any statements and/or representations that may have been made previously by either of them to the other are void and of no effect, and that neither of them has relied upon such statements and/or representations in connection with such Party's dealings with the other. The Parties expressly agree that it is their intention and covenant that (A) this Agreement, any performance under this Agreement, and all suits and proceedings arising out of, related to, in connection with or by reason of this Agreement, be construed in accordance with, and under and pursuant to, the laws of the State of Mississippi; (B) the laws of the State of Mississippi will be applicable and will govern any action or other proceeding that may be brought arising out of, related to, in connection with or by reason of this Agreement, to the exclusion of the law of any other forum; (C) unless expressly waived by Company, the exclusive jurisdiction and venue of any legal action with respect to the subject matter of this Agreement shall be the appropriate Court for Rankin County, Mississippi, and (D) each of the Parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such legal action. If it becomes necessary for any Party to undertake any litigation or to employ an attorney to assist such Party in pursuit of or protection of its rights under this Agreement, the non-prevailing Party shall be obligated to reimburse the prevailing Party for such fees and related costs and expenses, including reasonable attorney's fees, whether incurred at trial, on appeal, or otherwise. The invalidity, illegality, or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if such invalid, illegal, or unenforceable provision had been omitted. This Agreement shall not be amended or modified, and none of the provisions hereof shall be waived, except in a writing signed on behalf of the Parties hereto or, in the case of a waiver, on behalf of the Party making the waiver. All terms and conditions of this Agreement shall be binding upon the successors and assigns of the Parties hereto. No waiver of any provision of this Agreement shall be implied by any failure of either Party to enforce any remedy upon the violation of such provision, even if such violation is continued or repeated subsequently. No express waiver shall affect any provision other than the one specified in such waiver, and that only for the time and in the manner specifically stated. This Agreement may be executed in any number of copies, each of which shall be deemed an original and no other copy need be produced. Captions to and headings of the Sections and Paragraphs of this Agreement are solely for the convenience of the Parties and shall not be used for the interpretation or determination of the validity of the Agreement and/or any provision(s) hereof. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine, neuter, singular or plural as the identity of the person or persons may require.

COMPANY:

CUSTOMER:

LEC, INC.

A Mississippi Business Corporation

Name of Company



By: _____
Authorized Representative
(Signature)

Authorized Representative
(Signature)

Title

Leaders In Industrial Automation Control Engineering and IIoT Communication



Leaders in Industrial Automation
Control Engineering and
IIoT Communication



Our Applications

In the ever-evolving motion-control and electric motor industry, LEC's international experience in developing components, engineering systems and programming software for clients spans a vast array of verticals. Our broad client portfolio ranges from oil & gas, pipeline and transportation companies to water/wastewater, forestry and many more key industries.



Oil & Gas, Pipeline

- Drilling Rig Remote Monitoring Systems
- Production Monitoring Systems
- Pumping Unit Monitoring Systems
- Pipeline Metering Station Monitoring and Control Systems
- Pipeline Control and Block Valve Controls and Monitoring Systems
- Pipeline SCADA Systems



Water / Wastewater

- Wastewater Pump Stations
- Potable Water Well Controls
- Elevated Tank Controls
- Treatment Process Controls



Metals & Machining

- C-N-C Machining
- Arc Furnaces
- Punch Presses
- Rolling/Stamping/Slitting
- Die Casting
- Draw Blocks
- Annealing



Forestry / Agriculture

- Bucking, Sawing & Chipping
- Trimming, Sorting & Stacking
- Drying & Packaging



Power Generation

- Fuel Tank Farm Supervisory Control
- Process Water Filtration & Treatment
- Wastewater Filtration & Treatment
- Electrostatic Precipitator Controls
- Bottom Ash Control Systems
- Fly Ash Control Systems
- Hydro-Electric Generator Controls
- Raw Water Intake Controls



Robotics

- Pick & Place
- Welding
- Assembly



Communications

- Ethernet Networks
- VPN Access
- ControlNET
- DeviceNET
- Modbus / RS485
- Fiber Optic
- Cellular
- Internet



Monitoring

- SCADA Systems
- Remote Monitoring Systems
- Residual Chlorine Monitoring Systems



Automotive

- Tire Industry
- Welding Machines
- Component Assembly
- Automation
- Quality Control - Vision
- Inspection Systems



Plastics

- Injection Molding
- Extruding
- Blow Molding
- Thermoforming
- Ultra-Sonic Welding



Food & Beverage

- Batching
- Ovens
- Fillers/Seamers/Cappers
- Packaging
- Palletizers
- Bar Coding/Sorting



Chemical

- Custom Container Filling Stations
- Palletizers
- Batch Controllers



Paper Industry

- Paper & Pulp
- Converting
- Presses



Fiber Glass Insulation Production

- SMC Production
- 10 & 15 Ton Presses



Transportation

- Draw Bridge Controls
- Bridge Automation



Amusement & Entertainment

- Roller Coaster Automation
- Water Park Automation

LEC Is Engineering Smarter Systems

LEC supplies the competitive advantage to industry, turning challenging circumstances into revenue-generating results by providing the cutting-edge production and process management automation tools needed to face competitors head-on in a demanding global marketplace. Our proven experience is demonstrated via our clients' success in areas such as cost reduction, higher-quality manufacturing, process efficiency increase, greater employee safety and productivity improvement.



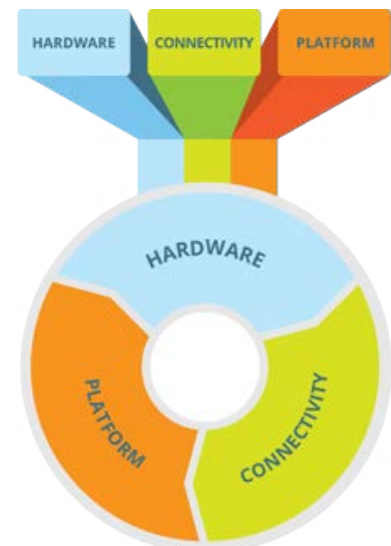
Who We Are

LEC provides industrial automation and control engineering, and industrial IIoT enablement and cloud platform services of the highest quality. Every day, we demonstrate an unending commitment to our clients, strategic partners and communities.

Automation is a crucial element of the manufacturing and production process. The efficiency of any process is dependent on successful system integration. LEC supplies the competitive advantage to industry, turning challenging circumstances into revenue-generating results. We provide the cutting-edge production and process management automation tools needed to face competitors head-on. LEC produces tangible benefits - cost reduction, higher-quality manufacturing, process efficiency increases, greater employee safety and productivity improvement.

Access to our professionals is not restricted to "traditional" business hours and workdays. Our highly experienced emergency support teams are available any time – day or night. By incorporating remote access features into your control system, our teams are enabled to diagnose issues, and in many cases remedy them from virtually anywhere.

Additionally, we offer our clients the option of attending customized training sessions, either on-site or in a hands-on classroom environment.



Proven Industry Leaders

Our passion is engineering smarter systems that exceed expectations. LEC's experienced and passionate team brings a multidisciplinary approach to addressing the challenges that affect our clients. We're setting a new standard in industrial automation control engineering and IIoT enablement.



Strategic Partner Alliances

LEC's well-established strategic alliances with industry leading component manufacturers, hardware providers, network carriers and platform developers enable our team to successfully design, produce, and integrate custom systems based on the specific, individual needs of each client. These Alliances play a vital role in LEC's consistent delivery of successful results.

Experienced Human Resources Behind the Technology

The core of our flexible workforce includes engineers experienced in a variety of disciplines with the knowledge to complete a project of any size and in nearly any industrial application. Our professionals are passionate about design, fluent with technology, and engaged in each aspect of every project.

- Automation Engineers
- Industrial Engineers
- Network Architects
- Electrical Engineers
- Mechanical Engineers
- Computer Engineers
- Civil Engineers
- Network Engineers
- PLC/Automation Programmers
- Certified Panel Technicians



Engineering Products & Services

Engineering & Consultation

Consulting services offered by LEC range from specification of a single system component to turnkey design-build services. We have an extensive network of resources, both technical and non-technical, which allows us to accommodate client needs during any phase of a project. These services are not specific to any particular market segment and are applicable to both public and private-sector projects. LEC provides the solutions needed as well as the documentation required to keep up with all details of a project; including schematics, hardware/software manuals, and fabrication details. All of our documents are accurate, easy to follow, and simple to modify.



Industrial Automation & Control Systems

LEC's team has decades of experience in engineering smarter automation systems for industry, delivering real solutions to successfully solve critical process and control application challenges. We are committed to the continuous training of our team and to the innovation advancement of our industrial automation services. Whether you need a single-station work cell, a completely integrated multi-functional assembly line, or the integration of new components into an existing system, LEC has the solution. Our team of experienced engineers, programmers, technicians, and software developers focuses on providing cost-effective solutions. Clients rely on us for process integration, machine design and build, PLC and RTU programming, HMI SCADA development, production monitoring and reporting, data collection, servo and VFD programming, machine diagnostics and alarming, panel design, and industrial IoT solutions.

Systems Integration

LEC's experienced team of control system integrators design and implement sophisticated control systems for manufacturing operations, process and other industrial facilities. We leverage our extensive knowledge of engineering, information technology, operations, and business to expertly integrate plant equipment to automate manufacturing and processes from the plant floor to the enterprise level. Automation helps manufacturers and processors reduce cost, increase production, use less energy and lower environmental impact. Our extensive experience with a vast array of hardware and software platforms and their unique communication protocols enables us to effectively integrate multiple machine control systems in accordance with specific client requirements, whether into a comprehensive control room, SCADA application, or cloud-based solution.



Engineering Products & Services

UL-508A Certified Industrial Panel Design & Fabrication

LEC specializes in providing custom control panel solutions of the highest caliber in the manufacturing industry with a proven track record of satisfying a variety of industrial automation needs. Our team of highly experienced technicians expertly construct control panels to the highest quality of industry standards using the best products from trusted hardware manufacturers. LEC's UL-508A Certified Panel Shop can accommodate any size project, and provide engineering support from design concept to completion.



Skid Design & Fabrication

Our engineers, technicians and fabrication teams provide the best quality skid-mounted measurement technologies and mechanical and electrical controls available in the industry. LEC's professionals can manage and advise on your project from initial design through start-up and commissioning. We offer both standard designs for quick turnaround to meet tight deadlines, and customizable solutions to meet unique regional or application requirements.



Programming

PLC Programming

Our skilled professionals provide software programming services for a variety of brands of Programmable Logic Controllers (PLCs). Our software development outcomes are easy to use, organized, and simplified, with descriptive comments to give our clients the information they need to maintain their equipment.

HMI & Operator Interface Programming

Regardless of the complexity of your HMI needs, LEC provides sophisticated, user-friendly systems that are easy to operate, and our professionals are experienced in designing and programming a wide variety of operator interface systems.

Motion Control Programming

We are skilled in the design, installation, and commissioning of an extensive array of motion-control components and variable speed drives, which provide smooth operation of electronic gearing, contouring, and circular motion applications.



Radio Frequency Controls

LEC has extensive experience in providing solutions utilizing a variety of wireless controls and I/O devices in accordance with your particular requirements. These are crucial when an application involves potentially dangerous machinery (such as conveyors and blenders) or the monitoring of equipment, motors and other devices from a remote location.

Programming

Industrial Internet of Things Enablement Products and Services

LEC offers experienced Industrial Internet of Things (IIoT) enablement, filling the gaps between disparate technologies.

- Integrating existing field devices and assets into a current IIoT framework.
- Connecting disparate systems into a single platform and user interface for monitoring and control.
- Developing ground-up, custom IIoT solutions to meet specific client requirements.
- Long-term solution support to ensure sustainability while meeting ongoing and future IIoT business needs.



Mission Critical IIoT Connectivity

- Highly secure and redundant wireless connectivity
- Advanced private network with client access to real-time network analytics
- Managed services staffed with skilled support and troubleshoot personnel
- Pre-commissioned hardware for optimized deployments
- 4G LTE Network
- System Consulting & Design
- Robust 24/7 ticketing system with solveIT™ support tool



Engineering the Components of IIoT

LEC offers experienced Industrial Internet of Things (IIoT) enablement, filling the gaps between disparate technologies. With years of industrial controls and automation experience, along with investment in new and innovative technologies and the brightest human resources, LEC is truly a market leader in deploying IIoT. Trusted by the industry, wireless carriers and enterprise clients alike, LEC is a proven partner in business.

Visualization & Control Through Robust IIoT Platform Technologies

- IIoT platforms delivering data visualization, analytics, and control
- Reliable alarm and fault notification systems
- Ability to extract data and enable control both remotely and in-plant
- Data logging and reporting functionality
- Simple configuration and intuitive user interface
- Access from any browser-enabled device



Introducing iQ2™. Intelligence. Squared.

iQ2 is LEC's complete, end-to-end IIoT platform solution, designed from an industrial automation engineering perspective, to effectively and efficiently address individual needs. Our flexible IIoT integration process quickly and easily enables our cutting-edge platform technology on the plant floor, for OEMs and any industrial remote assets.



ENABLING IIoT

Engineering the Components of IIoT



iQ Web SCADA

LEC's complete end-to-end monitoring and control solution, iQ Web SCADA, integrates into almost any new or existing control or automation system regardless of the function of the machinery, equipment, or system. The iQ Web SCADA platform can be used all or in part, depending on the needs of the user.



iQ CommSentry

LEC's iQ CommSentry service tool provides users with a simple solution to monitor and manage network performance resulting in reduced downtime and the prevention of costly errors. This platform simplifies compliance management, IP address management, easily tracks and locates network users and devices, and analyzes network traffic and bandwidth usage.



COMMSENTRY
MANAGING IIoT

Support



Technical Support Center

LEC's newly-launched, cutting-edge solveIT™ Technical Support Center provides clients with direct, 24/7 access to data, project information and support request updates using the latest technology compatible with today's browsers and mobile devices. solveIT™ is a user-friendly and highly-collaborative cloud-based system designed to give clients instant access to detailed information regardless of locale. solveIT™ features data sharing, client data input capabilities, support ticket tracking, project tracking, hardware information and much more, increasing overall project management effectiveness.

On-Site Support

Technical support is a crucial component of LEC's services, and we are always pleased to assist clients with on-site questions or maintenance needs.



Replacement Components

We have a commitment to providing every nature of support for our clients' systems throughout their service life. In addition to our remote assistance and on-site support services, we also offer replacement components for every aspect of control and automation systems.



**Leaders in Industrial Automation
Control Engineering and
IIoT Communication**

Appendix A

The State of Utah

In conjunction with NASPO ValuePoint

Attachment T

Utah Solicitation # CJ21-3

Technical Questionnaire

Subcategory O: Utility Operations, Monitoring and Support

SkyHawk Telematics



1 - General information:

Please provide a general description of the solution you are offering including:

a. Product Name

SkyHawk ConnectAnywhere

b. General Application Area

Subcategory O: Utility Operations, Monitoring and Support

c. General capabilities provided

SkyHawk's ConnectAnywhere web-based monitoring solution, which is hosted out of the AWS Data Centre, guarantees 99.9% service availability, 24/7 onsite support, automated system monitoring and dynamic resource allocation controls. For instance, as more network bandwidth, CPU, RAM, and storage are required, the system dedicates the necessary computing resources. Furthermore, the solution provides a separate, dedicated database, virtual server, IP address and SSL security. These dedicated resources ensure the highest level of performance and guarantee that the system is not degraded by other companies sharing the same system resources.

ConnectAnywhere allows unlimited user accounts or logins with Skyhawk staff providing the initial account setup and administration. Once the system is fully operational, clients have complete administrative IT access to the features and functionality of the system. The ConnectAnywhere solution provides complete GIS mapping integration and interface capabilities to other client software applications with REST API.

Some key features of the SkyHawk solution Include:

- The ability to obtain ECM engine data including fuel efficiency characteristics such as: Total Fuel Used (L), Fuel Rate (L/h), Instantaneous Fuel Economy (km/L), Average Fuel Economy (km/L) when available from the vehicle manufacturer.
- The ability to report on unsafe driver actions such as speeding (with local speed zone), harsh braking, harsh acceleration, etc.
- Alerts and alarms that are configurable and which can be delivered directly to users via email or SMS messaging.
- Unlimited number of user accounts (usernames and passwords) with complete administrator-level access and system control, multiple user access levels (e.g., Viewer, Manager, Admin, etc.) which are controlled by the administrator.
- The ability to create email and text contact lists per asset for real-time notifications.
- Map options default to Google, but access to client maps is available via an ESRI/GIS link.
- The website is protected with an industry- standard, 128-bit encryption with an SSL certificate, providing the ability to filter vehicles in real-time as well as the view of the data online.
- Custom Geo-Fencing and alerts on activity in and out of Geo-Fenced areas including Zoom-In, Zoom-Out, Pan, Drag- Zoom, Road Map Data, Air-Photo Data, etc. Access all reports in real-time online.
- Optional - Tablet support for in- cabin operations supporting advanced navigation and routing options.
- Optional - A completely integrated satellite asset tracking option for vehicles and for high-valued, non-powered assets.

d. Expected impact on cost/performance/functionality, etc.

We are proud to join our strengths in delivering industry leading and secure, Internet-based GPS tracking and management solutions to Power Utility organizations and advanced work truck sectors.

SkyHawk helps our utility clients with solutions for:

1. **Fleet Utilization** – Fleet Right Sizing and Productivity.
2. **Driver and Fleet Safety** - Reduced Speeding, Improved Driver Behavior, Reduced Motor Vehicle Incidents, Improved Operational Safety.

3. **Non-Productive Idle** – Reduced Fuel Usage, Reduced Maintenance Cost and reduced asset depreciation.
4. **Incident Investigation** – Recreate events as needed, improved cost/time/resources needs, improved insurance liability and compliance.

We do this using ConnectAnywhere™, our advanced cloud-based monitoring system, coupled with our suite of in-field data collection devices and applications. Our solution gives our clients detailed, real-time and historical data required to make the best operational and management decisions.

Our solutions are currently installed in over 5,000 vehicles for Hydro One Networks Inc. and are approaching 10,000 vehicles for Hydro-Quebec.

Please see a copy of a Utility Case Study recently completed for one of our utility clients.

- e. Subcontractors/partners involved in delivering service
For the purposes of this submission there are no subcontractors or partners required to deliver SkyHawk's service. If, as determined by the scope of work of each opportunity or client engagement, there is a requirement to work with or use contractors/partners, SkyHawk has the capability and capacity to do so. We have done so on multiple projects to date, as needed.
- f. Does the application that you are proposing have associated End User Licensing Agreements, and if yes, please provide.
Yes. See attached End User License Agreement (EULA)

2 - Turnkey Wireless Solutions:

- a. Strength and functionality of operational product as described

SkyHawk's ConnectAnywhere solution is a core platform used to offer our clients full oversight of their mixed fleets, assets and the underlying technology used to track, monitor and maintain core services that people depend on daily.

SkyHawk's Winter Operations GPS fleet management solution is unique in the industry, supporting a wide range of spreader controllers and sensors, and includes specialized winter ops reports. The solution effectively and efficiently deploys, monitors and manages fleets, drivers, assets and material usage.

Winter Operations managers have real-time and up to date visibility on the performance of drivers, current state of snow removal and other sources of information necessary to monitor overall operating costs, spreading frequency and quantities and to prove environmental and performance requirements.

Winter operations is where SkyHawk's Fleet Tracking platform stands out from the pack.

The SkyHawk solution integrates with a wide variety of computerized spreader controllers and whenever possible, pulls the actual material values from the controller itself, rather than performing a calculation-based estimate. ConnectAnywhere then has a wide variety of powerful Winter Operations reports available.

Hardware Highlights:
SkyHawk's hardware modems are non-proprietary and can be implemented on multiple AVL systems.
Modems have a 3-axis accelerometer to detect and indicate harsh acceleration and braking events in real time .
Modems have onboard, non-volatile, permanent memory capable of storing a minimum of one month's worth of data . In situations where communication is lost or interrupted, the collected data is stored and transmitted immediately once communication has been re-established by entering an area with cell coverage.

Modems report real-time events such as: ignition on/off, I/O state changes, harsh events, excess RPM and speed, etc.; reporting frequency can be every 1 second while moving or stopped and every 15-degree change in GPS heading. [Recommended default of 15 second reporting]
Hardware use true GPS signals for position and does not use assisted GPS positioning off cellular triangulation.
Hardware is remotely configurable over-the-air
SkyHawk offers modems that operate on the 4G LTE networks with 3G fall back with data transmission via TCP/IP connections.
Hardware is: - powered by the vehicle’s ECM data port (including OBDII, J-1939 Type 1/Type 2, and J1708), or the powered by the vehicle’s electrical system in such cases where an ECM port is unavailable - designed to withstand typical power surges that may occur within a vehicle’s electrical system - operates on 6 to 36 volts with no voltage regulator or converter added to the power line
Modems have Wi-Fi and Bluetooth wireless connections. Wi-Fi provides Internet access via cellular data connection. Wi-Fi is configurable with defined SSIDs and passwords. Wi-Fi is also configurable to not broadcast SSID.
Modems have the options of being installed within a tamper proof case.
Modems collect and transmit data from a growing range of spreader control systems
Modems tracking of blade position using one or a combination of Plow Blade Proximity Sensor, Hydraulic Pressure Sensor and IONS Electric/Air Over Hydraulic Sensor to ensure clients get accurate plow positing reporting .
ECM cables are direct cabling with no 3rd party hardware inline between the AVL modem and the vehicle ECM port. Connects to OBDII, J-1939 Type 1/Type 2, and J1708.
Modem operating temperatures from -22°F to +158°F with a humidity of 95%.
Wireless Capabilities: Certified on all major carriers (AT&T, Verizon, US Cellular, Sprint). Modems can utilize different cellular carriers, depending on the region, to provide the best available coverage for the entire fleet.
Select Modems interface with IP enabled dash cameras to provide image transfer to ConnectAnywhere.
Select modems utilize a windshield mountable GPS and communications antenna to reduce tampering. All antennas and cables are suitable for simple and permanent vehicle mounting without affecting other vehicle components or operating systems.
SkyHawk offers modems that have a backup battery used for detection of loss of GPS or power. ConnectAnywhere software can send alerts via SMS and email to selected contacts when tampering is detected.
Cloud Based Application: ConnectAnywhere
ConnectAnywhere software utilizes Google Maps as its base mapping view and is officially licensed as SkyHawk is a certified Google partner . ConnectAnywhere also has a search function to easily find vehicles, assets, geofences, and landmarks . Maps can be viewed as Satellite, Terrain, Hybrid, and Street Level. Also tracking provides a breadcrumb trail showing each timestamped movement of the vehicles.
ConnectAnywhere is a secure cloud web-based solution for remote configuration, management and update series for the maintenance of GPS telematics. Vehicle positions and status automatically update on screen without any input from the end-user.
Asset tracking data is not routed through any country other than Canada, and the cloud-based servers are physically located in USA .
ConnectAnywhere has a complete screen refresh within 15 seconds and generates reports within 3 minutes for an end-user using any modern Internet capable device and web browser.
End-user system access is available 24/7 (24 hours 7 days a week) via any web browser connected to the Internet

The system is capable of showing, in real time, the Automatic Salt Control (ASC) data , as well as generate suitable reports based on available spreaders. This data includes such things as set/actual rates, total material dispensed as well as trip and/or seasonal totals.
ConnectAnywhere has the ability to organize vehicles, employees and users in a multi-tier organization . It offers the ability to report performance metrics rolled-up at different hierarchical levels and the ability to drill-down and across the hierarchy to investigate trends and anomalies .
ConnectAnywhere supports user-configurable vehicle identification .
Information data stored by the SkyHawk is accessible on-line for a period of up to two years and maintained in a data warehouse beyond two years. Data is accessible by request for a minimum of 7 years or the lifetime of the contract (whichever period is longer) without additional cost. Data older than 7 years shall be made available by request on compatible data storage devices. The maximum latency period between the most recently collected data and the time that it is entered into the data warehousing system is no more than 30 seconds and no more than the normal latency afforded by the network being used.
Geofences can be created within ConnectAnywhere via a simple drawing tool. Geofences can be assigned to specific vehicles or the entire fleet. Geofences can also be public or private to specific users. Alerts can be set up to notify users upon an asset entering/exiting geofences . Finally, specific geofences can be setup as "Storage Depots" wherein <u>salt that is offloaded from the spreader is not included in our salt reports</u> , allowing the users to have an accurate reflection of the amount of salt dispersed on the roadways over a specified period of time
Data is backed up daily.
ConnectAnywhere provides an unlimited number of user accounts and contacts (i.e. <u>no "per user license"</u>).
ConnectAnywhere has the ability to track up to 10,000 vehicles in real-time , with all vehicles viewed at the same time.
ConnectAnywhere utilizes SSL (Secure Socket Layer) internet security (i.e. accessible via https).
ConnectAnywhere is not limited to a specific browser or version (Google Chrome, Internet Explorer, Safari, Firefox, etc.).
ConnectAnywhere supports GIS/ESRI data and application integration and mapping with the ESRI connection such that maps can either be hosted, or preferably, linked to the client's ESRI database so that when changes are made, they are made on the mapping platform for the AVL at the same time.
ConnectAnywhere has end user full administrator rights for: • Adding/editing user accounts and asset contacts • Easily managing account privileges and profiles across all user groups • Input/output configuration and labeling • Hardware setup and management for AVL, satellite asset tracking and lone worker/personnel tracking • Complete asset management including renaming, hardware and contact assignments.
ConnectAnywhere has the ability to create and manage public and private geofences .
ConnectAnywhere has the ability to integrate with client or third-party server infrastructure to extract and display photos and/or video captured by a dash camera within a vehicle.
The primary display of ConnectAnywhere is a computerized map view in real time of the entire fleet and the most recently communicated status of vehicles. The map includes highway identifiers including other linking roads. Vehicle icons rotate to display proper movements and direction of travel .
ConnectAnywhere has the ability to incorporate weather data into the map layer from client's contracted weather services vendor.
ConnectAnywhere can display tracings of the vehicle movements in real-time on the road map; this map accurately represents the department's base map and any other significant geographical features.

ConnectAnywhere provides scheduled reports to be delivered at user-defined intervals and formats.
Reports are printable and can be exportable into Excel and PDF reports. Please see Appendix for samples of the reports available.
A public access site can be created and customized for public viewing - to allow citizen tracking (read-only map displaying vehicles in real-time or with a lag for safety reasons)
Ability to deploy portable devices for GPS tracking of contractors and rental equipment
SkyHawk provides seasonal deactivation for units that are not in use wherein no carrier fees are charged, and the ConnectAnywhere fee is reduced to a suspension fee.
ConnectAnywhere Reports:
SkyHawk's ConnectAnywhere standard reports include: History Report, Materials Admin Setup, Vehicle Trip Report, Fleet Status Report, Vehicle Detail Report, Long Term Parking Report, Inputs Report, Spreading by Speeding Report, Harsh Events Report, Speeding Report, Input Based Speeding Report, Geofence by Vehicle Report, Geofence by Geofence Report, Route Activity Report, Winter Operations Trip Report, Route Service Report, DLA Report, Malfunction Indicator Light, Winter Operations Material by Time Report, Winter Operations Material by Geofence Report, Sweeper by Geofence Report, Dust Control Report, Fleet Utilization Report, Non- Productive Idle Report. Please see Appendix for samples of the reports available.
The Route Activity report displays routes, the portion of a route, or combination of routes, that has been plowed, had material applied, travelled, swept, or has had a combination of these attributes completed (i.e. which roads have been both plowed and salted).
Users can run the report for current or historical data.
Roads that are completed are color coded, the color fades with time, to show white if the road had been completed over the designated time interval. Routes can be directional.
This report also shows the percentage of the route that has been completed over the selected time interval.
The Winter Operations by Trip report displays the amount of material dispersed by a vehicle over a given period of time. (Note: The end of the trip material offloaded at the depot from the spreader vehicle is not included).
The Material by Time report shows the operational costs, labor costs, fuel costs and material costs incurred over a winter event across the entire fleet of vehicles.
The Route Service report shows the streets that have been plowed and the streets that have had material applied over a live map view.
The Input Speeding Report shows events where a vehicle has exceeded a selected speed when an input such as a plow is down, or sweeper broom is on.
The Material Speeding report shows events where a vehicle has exceeded a selected speed when a spreader is dispersing material.
ConnectAnywhere has a Fleet Utilization report for all vehicles within a fleet, showing the engine hours, odometer, the amount of fuel used, the run time, and idling time.
The Malfunction Indicator Light (MIL) report shows all active ECM trouble codes across the fleet of vehicles.

b. Applicability to government needs

SkyHawk has delivered advanced telematics solutions to a mixed fleet, including winter operations functionality, for more than 7 years, to clients in the USA as well as Canada. Our continued focus is on being the industry leader in this sector and in working with our clients has produced functionality which includes:

- Integration with most major material spreader controllers,
- Cost-based reporting for material usage,

- Winter operations trip & material usage reports,
- Public winter ops site,
- In-cab route optimization,
- Route navigation and return-to-route,
- Route activity reporting,
- Blade wear report,
- Spreader speeding,
- Direct liquid application (DLA) reports, and much more.

As an end-to-end solutions provider, with a proven track record of successful client partnerships, we understand the needs of complex deployments such as those defined by the State of Utah in conjunction with NASPO ValuePoint. As such, we are fully committed and confident in our ability to provide a solution that not only meets but exceeds the goals, objectives and responsibilities that would come with this relationship. To support our belief in that ability, below are some components that we feel fully support the project scope as defined in this RFP.

Experienced and competent subject matter experts: SkyHawk has a team that has successfully delivered similar projects of scope and scale. SkyHawk's team includes senior management/corporate project sponsors, sales account managers, project management specialists, operations/procurement/order fulfillment staff, installation teams, support staff, and financial/billing specialists.

Project Management: Effective management is vital to the overall success of any project, and SkyHawk has proven its ability to deliver telematics projects to complete vehicle and feature roll with very large and complex projects.

Project Management Approach

Skyhawk's Project Team utilizes the Project Management Institutes (PMI) project methodology phased approach that is broken down into five (5) process groups: Initiate, Plan, Execute, Monitor and Close. In each process area, we have identified key documents and tools to serve as inputs that result in deliverables for each phase.

SkyHawk's project team will spend a considerable amount of effort on detailed requirements gathering to ensure a complete understanding of the organization's needs and will compile a comprehensive Project Plan which we feel is critical to the project's success. The Project Plan will be updated regularly as the project progresses, and will establish project roles and responsibilities, a detailed schedule of tasks, Quality Plan, risks, and Change Control. Additionally, SkyHawk's project team will work with your project team in preparing a full updated project schedule, including the installation schedule. Bi-weekly status meetings will be held to review the project schedule and to review any open issues in SkyHawk's JIRA ticketing system.

Project Communication

Project Communication can be established in the form of regularly scheduled project meetings with status reports issued weekly. The status report will contain at a minimum the following information:

1. Dashboard view on the progress of installations, tracking completed installs to planned
2. Task / Action Item List from previous meetings
3. Defect /Issue Log generated from the Jira Ticketing System
4. In addition, SkyHawk will collaborate with ODTO on preparing awareness communications for ConnectAnywhere training, hardware installation training, etc., as appropriate.

Communication Plan

The Project Communication plan will be created in partnership with SkyHawk and the State's Project Managers to outline how the AVL project team will be communicated during the project.

The Communication Plan shall be completed early enough in the project to be included for review at the Project Kick-off Meeting. Communications include but not limited to; status, meetings, issues, deliverables access, and design/document reviews.

Reporting Methods

SkyHawk, in collaboration with the State's project team, shall determine reporting and communication cadences. During the project implementation phase, the Status Report will be issued weekly or bi-weekly, prior to the Project Team Meeting. The Status Report will contain percentage complete and dashboard views of scope, schedule, cost, and quality. It will be prepared in formats approved and will contain at a minimum the following information:

1. Progress Dashboard showing percentage complete from previous meetings
2. Defect Log generated from the Jira Ticketing System
3. Project Status as it relates to the Work Plan
4. Deliverables status
5. Planned activities for the upcoming two (2) week period
6. Future activities
7. Requirements Traceability Matrix (RTM)
8. Report and remedies in case of falling behind Schedule
9. User Acceptance Test Feedback
10. Risk/Action/Issues/Decision (RAID) Log

Solution Configuration

SkyHawk's "ConnectAnywhere" solution is the result of our unwavering commitment to our client partners to provide them the data they require to make informed decisions to maximize operational efficiency, minimize environmental impacts, and protect the safety of both employees as well as the general public. Through continual consultations with the people responsible for the wellbeing of municipal, provincial, and state fleets and the roadways on which they operate, we have incorporated the feedback of these industry experts, along with the lessons we have learned along the way, to the data we collect and the information we report.

To accommodate the ever-increasing volume and diversity of data sources we pull from, the latest version of ConnectAnywhere is architected using modern design techniques that allow us to support many thousand simultaneous connections while maintaining flexibility. This provides us the capability to add or modify the underlying data of ConnectAnywhere to support new feature development without the complexity and downtime that would be required in a more traditional relational database environment.

This flexibility also allows us to support a wide variety of data collection devices, including multiple models of spreader controllers, telematics modems, asset trackers, etc. which enable us to provide a "right-sized" solution for the highly diverse fleets our clients maintain. We also promote "configuration" over "customization"; when we are presented with a business problem to address for one of our client partners, we approach the solution in such a way to benefit all of our users, with consultations as necessary, and make the additions available to our entire client base with the capability to adjust parameters to suit their own operational needs

The client onboarding process involves our project team gaining a thorough understanding of your business requirements, which is then used in the setup of your ConnectAnywhere portal. Starting with the master vehicle list, we meticulously review every vehicle and the data points to be collected from each, including such items as the ECM type, spreader controller, discrete inputs for plow blade position or beacon light monitoring, etc. This is then entered into ConnectAnywhere, which allows us to normalize the potentially many different sources into the consistent user experience in terms of display and reporting. From there, we can adjust the vehicle messaging profile and event thresholds to suit your business goals.

We also work with you to gather the user account information to create the "account templates" that control the functionality and subset of assets that each end-user has available to them. Other key configuration items include the setup of system alerts and scheduled reports.

Specialized Solution Offering: When dealing with a complex fleet of mixed vehicles with specialized reporting functionality (e.g. winter operations) it is very important to acquire a solution that is designed and built for the vehicle types and operations of a large municipal organization.

SkyHawk's ConnectAnywhere telematics solution has been designed and built specifically for this application and supports the specialized and advanced functionality required to more effectively and efficiently operate the services of your organization.

Vendor solution engineering/customization: While having specialized and feature matched system functionality is very important it is also important to have a telematics vendor that has the resources and capabilities to perform solution engineering. Your organization may likely have requests and requirements which need custom development and attention to properly integrate with existing technologies and systems, including data exchange with other software applications. This cannot be achieved with "out-of-the-box" functionality.

SkyHawk has a team of solution specialists and software engineers that are capable of performing such tasks. Your organization will have direct access to the Company who owns, designs and develops the solution and NOT a solution reseller.

Installation Plan/Staff: Vehicle installations and testing are one of the most critical parts of any telematics system. At SkyHawk we refer to it as the "foundation" upon which all other functionality is built or layered. A well-designed installation plan along with a team of reliable installers is required for success.

Furthermore, it has been the experience of SkyHawk that best results are achieved when a combined approach of vendor/contracted installers working in conjunction with the City's mechanics and technical staff is utilized.

Effective Communications Plan: Engagement of your staff and departments to obtain a deep understanding of goals and objectives, as well as obtaining input, feedback, and required "buy-in" from management, system users and stakeholders leads to a better managed and implemented solution. This is best accomplished with an effective communication and engagement plan which starts before implementation begins and carries through all project phases.

SkyHawk has significant and relevant experience working with large clients in delivering successful communication plans. Our Project Team is built of experts in the deployment of AVL projects. They are motivated by excellence and have the combined skills and capabilities to deliver the project on time and on budget and of the highest quality.

c. Number actual turnkey systems as proposed or similar to proposed system currently in successful use.

Provide references

SkyHawk attributes a significant portion of our success to the belief that our client relationship is a true partnership. We take a proactive approach to working with our clients and they have been instrumental in the design of our solutions. Our clients motivate and challenge us to constantly seek to develop and refine our technology. As we continue to grow and expand, SkyHawk will continue to seek input from our clients to allow us to continue to advance the telematics industry with innovative solutions. Additionally, SkyHawk remains committed to providing a high level of service throughout every layer of every project.

The SkyHawk client size ranges from enterprises account to small municipal governments. Our solution is currently installed in +5,000 vehicles for Hydro One Networks Inc, +900 vehicles for the Iowa Department of Transportation, +900 vehicles for Nova Scotia Department of Transportation, currently rolling out 10,000 units with Hydro Quebec.

The following are a sampling of some governments clients that currently use the SkyHawk solution:

City of Portland, MA	North Dakota DOT
Town of Davenport, IO	Nova Scotia DOT
Town Urbandale, IO	County of Grande Prairie, AB
Rochester Hills, MI	City of Red Deer, AB
Midland County, MI	Federated Co-op, SK
Muskegon CRC, MI	Manitoba Hydro, MB

Midland CRC, MI	City of Hamilton, ON
City of St Clair Shores, MI	Hydro One Networks, ON
City of Kalamazoo, MI	Town of Flat Rock, NL
Stark County, OH	Hydro One Networks Inc., ON
The city of Brunswick, OH	Municipality of Chatham-Kent, ON
City of Joliet, IL	Hydro-Quebec, PQ
City of Springfield, MO	Town of Quispamsis, NB
City of West Fargo, ND	Town of Rothesay, NB
City of Pittsburgh, PA	Town of Dieppe, NB
City of Mount Pearl, NL	Portugal Cove-St. Philips, NL

Our references below will attest to SkyHawk's ability to deliver a superior product on time and in scope.

Reference (1)

New Hampshire Department of Transportation

7 Hazen Drive Concord, New Hampshire 03302-0483

David Gray

Winter Maintenance Program Specialist

(603) 485-3806 ext. 324

dgray@dot.state.nh.us

October 2016

Ongoing Project

GPS/AVL Winter Operations Solution. 65 Winter Operation Vehicles, and 24 Pickup Trucks - 89 Units

\$272,072.66

Reference (2)

City of Pittsburgh

414 Grant St. Pittsburgh, PA 15219

Chris Belasco

Project Manager

(412) 400-4505

chris.belasco@pittsburghpa.gov

October 2018

Ongoing Project

Complete Telematics Solution, Route Optimization, and Route Navigation system. 138 winter vehicles with a mix of approx.

350 heavy and light-duty vehicles - 488 Units

\$1.5 Million

Reference (3)

City of Hamilton

71 Main Street West, Hamilton, ON L8P 4Y5

Angela Storey

905-546-2424 ext. 6483

Angela.Storey@Hamilton.ca

April 2016

Ongoing Project

EMS vehicles that required integration with Bluetooth, Garmin devices for in-cab communication with Central Ambulance Control Centre and Ministry of Health and Long-Term Care reporting system as well as PTO reporting for lights, sirens.

Roads & Maintenance vehicles - design and creation of a Public access website, a mobile app for contractor specific

application, integration to spreader controllers, and PTO status for winter snow plows.

Simple track and trace for Parks and Recreation, Animal Services, Buildings, By-laws, Cemeteries, Forestry, Hamilton Water, Horticulture - 750 Units to date.

\$5 Million

Reference (4)

Hydro One Networks Inc.

6975 Kenderry Gate | Mississauga, Ontario L5T 2Y1

Frank Currie

Manager - Fleet Services

(905) 696-7190 x 3315

frank.currie@hydroone.com

October 2013

December 2016

SkyHawk Telematics provided Hydro One with a complete telematics solution that facilitated fleet monitoring for multiple lines of business including Construction Services, Forestry, Provincial Lines, Fleet and Station Services. Over 5000 vehicles were installed with a dual-mode cellular/satellite solution to equip its fleet comprised of the boom truck, off-road and light-duty vehicles. The hardware installation and testing was a joint effort between the Hydro One mechanics and SkyHawk technicians, taking approximately 22 months to complete.

\$20 Million

Reference (5)

City of Davenport Iowa

226 West 4th Street, Davenport, IA52801

Art Bartleson

Director of Public Works Street Maintenance Supervisor

(563) 327-5114

abartleson@ci.davenport.ia.us

December 2015

November 2016

Installed SkyHawk 4G GPS/AVL system in late 2015 to replace an existing 2G system from another vendor. Davenport monitors their salt spreaders equipped with FA5100 and FA6100 controllers, graders, and supervisor vehicles. They use the live "Route Service" mapping overlay to monitor winter operations. SkyHawk has developed a printable route completion report for drivers coming on shift; testing at Davenport and other customers is helping developers maintain a timeline for an early fall release. City snow operations staff use SkyHawk to manage material usage, report costs and improve efficiency. Waste Department on boarded 2020 with 31 garbage trucks.

\$82,000.00

d. Overall interoperability of turnkey system for government use

SkyHawk's strength is in its ability to meet the needs of a very diverse fleet, such as governments require. Our current client portfolio includes large cities, municipalities, utility companies, construction companies as well as simple delivery vehicles.

The modems we offer have a robust set of features with reliable track records, including standard store- and-forward capabilities for when the vehicle is out of cellular coverage, as well as the ability to receive and perform over-the-air (OTA) configuration or firmware updates in the field.

This eliminates the need to physically visit the vehicle for support and maintenance. SkyHawk's most widely used modems range from simple track and trace to the most complex of applications used for optimal winter maintenance tracking.

e. Accessories available for turnkey offering

In addition to SkyHawk's flagship product ConnectAnywhere, the following accessories are available for easy add-on functionality:

Route Optimization

SkyHawk partners with Quetica to offer a Route Optimization solution for our clients. Route optimization is a mathematical analytics approach that uses sophisticated optimization algorithms and big data technologies to find the best solutions. Examples of optimization applications in business include determining best routes, schedules, capacity, and pricing to maximize return on investment from materials, labor and equipment.

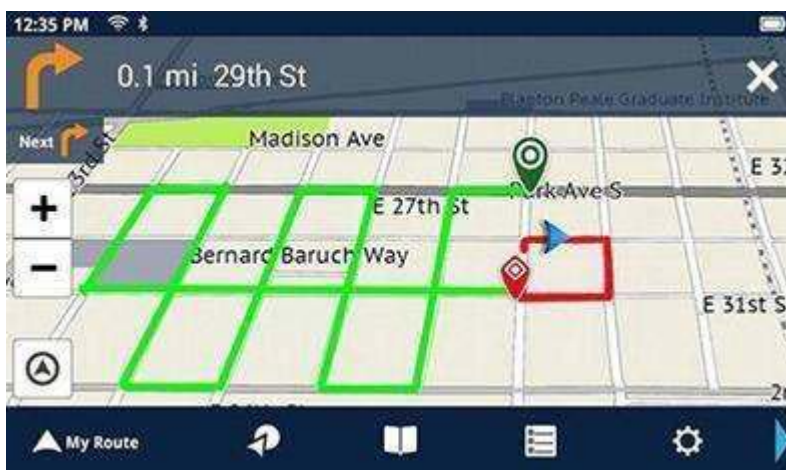
In-cab Turn-by-Turn Navigation and Routing

In cab, turn-by-turn navigation is offered through our partner Magellan. Utilizing the Magellan RouteComplete System. RouteComplete allows administrators to easily pre-schedule, adjust and update routes over the air from the back-office. All routes are loaded on the device allowing route change to be sent to the drivers. RouteComplete was designed for route planning in complex, highly dense urban canyon environments where accuracy can be a challenge. RouteComplete includes Return-to-Route advanced features such as Locked-on-Route, Deviated-Point-Navigation, Event-Driven Re-Routing, High Accuracy GPS, Real-Time Route Completion Monitoring and Real-time Route Management.

The driver can use the tablet touch screen to identify areas where they cannot proceed and identify the issue (temporary road closures, double parked cars, construction, etc.). The tablet navigation software will then navigate the driver to the closest area where they can resume the route. The administrative portal will display these areas on the map display for all routes.

The in-cab tablet provided is the Magellan Kiron Tablet, specifically designed for use inside a Winter Operations vehicle. The tablet is a touch screen, ruggedized, with voice commands that can easily be heard in loud environments. The tablet comes in two versions, an LTE version that utilizes its own sim card for data transmission, and the Wi-Fi version for connecting to a SkyHawk modem and utilizing the modem hotspot for data transmission.

The tablet can be unlocked for use with other applications and email; however, it is an Android based tablet, and The Route Complete System is currently only available on Android based devices.





SkyTrak Mobile App – Driver & Vehicle Tracking

SkyTrak is a mobile app that provides a simple and cost-effective telematics solution for tracking temporary workers, leased vehicles, and contractor fleets. SkyTrak may also be used in a standalone fashion as the primary means to monitor a customer's fleet.

The SkyTrak app is available free of charge from either the Apple App Store or Google Play. The SkyTrak app provides rapid, almost immediate deployment to provide a set of features in ConnectAnywhere. SkyTrak relies on a smartphone's existing cellular or Wi-Fi connection provides a zero-acquisition cost solution to basic fleet tracking.

There is a monthly fee for accessing the data on the ConnectAnywhere site. SkyTrak will not function unless a valid user account and list of vehicles is created for the app user to sign in and use.



Designed for ease of use and simplicity for the operator, the app only requires the driver to identify themselves (through login) and select the vehicle they are driving. Subsequently, start and stop buttons enable and disable tracking respectively.

The app currently provides the following functionality:

- Live GPS tracking
- Driver ID
- Route servicing
- Reporting
- Contractor payment reconciliation
- Contractor sub-account access

SkyHawk plans to further develop the app by integrating additional onboard sensors. Chief among these are retrieval of engine diagnostics and other information through the use of inexpensive and readily available off the shelf OBD2 Bluetooth adapters, and specialized salt controller data and digital inputs.

PlowTracker Public Website

The SkyHawk Telematics PlowTracker public website is designed with the following features:

Display Client's winter vehicles (equipped with SkyHawk Telematics AVL) current position on Google maps for public viewing. This feature does not display routes. Clients can decide which vehicles are shown on the public site by selecting them via the "Public Site" menu option.

PlowTracker shows Municipal and contractor plows working together to clear roads. On other days, or if a significant snow event is forecast, Plow Tracker may show Municipal plows doing preventative winter road maintenance such as using salt and brine to keep the roads clear of ice.

The system provides a configurable delay for vehicle position (i.e. 5 min delay). This feature is designed to add some protection for the Operators as displaying live data may allow the public to intercept trucks and interfere with standard plowing operations. The delay is configurable to any number of minutes via the "Public Site" menu option. The timed delay can be disabled by setting the delay status to 0.

There is a minimum speed configuration option. If vehicles are travelling below a specified threshold the selected vehicles will be hidden to the public. This can also be disabled by setting the minimum speed to 0.

The public can select how much previous data they want to view either 2, 4, 12 and 24-hour periods. The screenshot below shows a bread crumb trail of routes completed in the past 4 hours as per the selected time frame.

Public Website

The public will have viewing rights to the vehicle icon only; vehicle id, driver ID, or speed is not displayed.

Clients have the ability to overlay with specific layers including MTO camera system. The site can be configured with a geographical "boundary". Any messages, vehicle icons that occur outside this boundary will not be shown. The user has zoom in/out functionality on the Google Map.

Driver ID – Key Fob



Each driver gets a unique key fob, required for each journey, and a key reader to ID drivers is installed on the vehicle's dash along with our GPS tracking unit. When the vehicle is turned on, the driver presents the key fob into the key reader.

I-Button Reader Assembly (Includes Reader, key fob, jBuzzer, 4-wire)

Enterprise Level and Third-Party Integrations

ConnectAnywhere uses a REST API to easily integrate into third-party applications. The REST API provides simple read-only access to the most important data items in the ConnectAnywhere database: assets (both static attributes and current dynamic state) and messages (data points or transactions). It is an HTTP-based interface implemented using REST (Representational State Transfer) principles, intended to be used by application developers who wish to transfer asset and message data to third-party systems or data management tools. By using JSON and HTTP/HTTPS the API can easily be accessed by an application using any of a variety of languages.

f. Thoroughness of the vetting process used to select partners

SkyHawk owns and has designed and built the cloud-based telematics software solution ConnectAnywhere, however a technical partner ecosystem is utilized for various aspects of our solution including the cloud-hosting, database managed services, mapping interface, in-vehicle data collection and communications hardware as well as interfaces to other third-party software applications as may be required by the client.

SkyHawk's partnerships, which support our main ConnectAnywhere cloud-based application, mainly consist of large, leading enterprise-based organizations such as Google, MongoDB and Amazon (AWS). The other major component of our technical partner ecosystem includes companies that provide physical hardware included telematics modems, cabling, and sensors that collect and transmit data from the vehicles. To ensure we are not exposed to any major supply chain issues, (including those caused by COVID-19) SkyHawk holds a significant inventory of most all its major components for rapid and easy distribution to our clients.

Our success with partnering is demonstrated in the City of Pittsburgh example. As part of a public bid award, SkyHawk partnered with Quetica LLC, and Magellan Solutions to provide the City of Pittsburgh with a complete Telematics Solution, including Route Optimization, and a Route Navigation system. 138 winter vehicles were installed in Phase 1 of the project during Q4 2018, with a mix of approx. 350 heavy and light-duty installed during Phase 2 of the project in Q4 2019.

As for the vetting of these partnerships, anything development-related is trialed, tested, and proven for our needs wherever possible by our development team before releasing to our clients. The same is true for our hardware solutions.

We have a hardware department that ensures the solution we recommend works, especially for each client's needs and specific environmental conditions.

g. Thoroughness of the process used to test the integration of the components in the solution and ensure the functionality of the overall solution

SkyHawk will provide installation technician(s) who shall provide installation services, installation training and hardware troubleshooting services to the client during the hardware installation rollout. The SkyHawk appointed PM will collaborate with the client on installation locations and logistics at the client preferred locations. SkyHawk will provide the sub-contractor with a suitable quantity of spare parts for service calls so that they can complete most minor repairs on the first visit.

Sample AVL Validation Checklist

This form is to be populated by the installer and a scanned copy is to be submitted to SkyHawk for record and reference.



AVL Validation Checklist

GENERAL INFORMATION			
Client Name	City of Mississauga	Vehicle Number	
Vehicle Make/Model/Year			
Odometer Reading	☐ Miles ☐ KM	Engine Hours	
ECM Type	☐ OBD2 ☐ J1939 Type 1 ☐ J1939 Type 2 (Green Connector) Other:		
Modem Type / Serial #			
Spreader Make / Model			
Driver ID Enabled	☐ Yes ☐ No	WiFi Enabled	☐ Yes ☐ No
CONNECTANYWHERE - BASIC TEST RESULT CHECKLIST			
Item	Test Procedure (indicate ☒ for Pass, ☐ for Fail & record notes on failure)		✓
GPS Position	Search for the vehicle using the ConnectAnywhere Asset List , verify location on map is correct and it is showing correct date and time		
Ignition On/Off messages	Cycle engine - Review History Report for Ignition On and Off messages		
Odometer/Eng Hrs reading	Verify the History Report displays correct odometer and engine hour readings		
ECM Data (if applicable)	Export History Report into Excel, verify VIN & other engine data is displayed		
Driver ID (if applicable)	Turn vehicle Ignition On , scan the Driver ID Fob/card to authenticate on the system, verify the Driver ID is displayed in the History Report & mouse over		
Spreader (if applicable)	Set a spread rate on the controller, verify in History Report the set rate selected and actual rate is displayed. Ensure accumulated totals for weight and distance increase.		
Idle Time	Ensure vehicle has been Idling for greater than 5 minutes, turn ignition off and verify the History Report displays correct idle time		
INPUT TEST RESULT CHECKLIST			
Input Test Procedure: Change the status of the Input from Up/Down, On/Off or In/Out and verify the correct status is displayed by refreshing the History Report. ☒ = Pass ☐ = Fail			
Input	✓	Input	✓
Front Plow		Right Boom	
Wing Plow		Left Boom	
Belly Plow		Centre Boom	
Beacon 1 (indicate color)		TO	
Beacon 2 (indicate color)		Boom	
		Other (list):	
		Other (list):	
		Other (list):	
		Other (list):	
		Other (list):	
TESTER SIGN OFF			
Notes: Record any failures or anomalies with the vehicle and call the SkyHawk Support Desk for assistance troubleshooting.			
Spreader Controller Calibration:			
Tested By		Date	

NOTE: The system will not function correctly if tested inside a building. Ensure to test when vehicle is parked with clear view of the sky, away from buildings or the tree line.

Please scan and email the completed form to your SkyHawk Telematics deployment representative.

For assistance with testing or troubleshooting call the SkyHawk Telematics Support Desk at 1-844-424-7759, Option 2.

V1.0 - 2019-11-27

Troubleshooting and Configuration Changes

The SkyHawk Support Desk will assist the Customer with troubleshooting malfunctioning hardware devices. If the device can't be fixed through Over the Air (OTA) configuration changes, manual reprogramming, or additional diagnostic measures, the SkyHawk Support Desk will recommend either returning the device to SkyHawk for repair or dispatch a field technician for a service call.

The Customer shall contact SkyHawk Support Desk when making the following configuration changes:

- Baseline odometer or engine hour value

- ECM type
- Change to vehicle voltage of AVL modem device
- Change to installation method of AVL modem device (3-wire, hardware ignition only, or ECM power)

Installation, Removal or Repair of Hardware

The Customer shall contact the SkyHawk Project Manager or SkyHawk Support Desk to schedule a service call if a unit is to be removed, installed, or needs repair. SkyHawk will dispatch a trained, qualified service technician to the Customer site. SkyHawk technicians are equipped with a small stock of commonly used spare parts so they may complete a repair during the same service call as the initial troubleshooting. Equipping our Service Technician with spare parts results in both time and cost savings for the Customer.

Ordering Hardware

The Customer shall contact their SkyHawk Account Manager to place an order for hardware. A quote will be provided for the Customer's review and approval. A P.O. is required from the Customer to authorize the purchase.

Winter Hardware Validation Testing

SkyHawk will assist the Customer with training and a test plan to efficiently conduct its own Winter Hardware Validation Test to ensure the winter equipment is re-installed correctly and operating as expected. This test is encouraged every fall before the start of the winter season. SkyHawk can also provide trained technicians to conduct the test for an additional fee.

Return Material Authorization (RMA)

The Customer shall contact the SkyHawk Support Desk to obtain authorization before returning any defective or un-used hardware. The SkyHawk Support Desk will respond in writing with the RMA number, return address and instructions for preparing the courier documents.

Discontinued Hardware

When a hardware device is going to be discontinued, the SkyHawk Account Manager will notify the Customer in writing of the discontinued product and will provide as much advance notice as possible. A suitable replacement will be recommended by the Account Manager with an accompanying price quote. The SkyHawk Support Desk will provide an installation guide and assistance to install the new device for a demo period or can arrange for a service call to have the new device installed by the SkyHawk-approved installation sub-contractor.

Communication

Regularly Scheduled Software Release and Maintenance Update

The SkyHawk Support Desk will notify key personnel of the Customer via email five (5) business days in advance of an upcoming Software Release and Maintenance Update. The first notice will include the date/time and approximate duration of the maintenance window. A reminder email is sent the day of the update and this notice will include the release notes. Once the update is complete, the release notes can also be found on ConnectAnywhere under the Help menu.

Service Interruption or Unplanned Outage

The SkyHawk Support Desk will notify key personnel of the Customer via email as soon as possible when any service interruption or unplanned outage of the software is detected. The Support Desk will continue to provide regular updates via email until the issue is resolved.

Annual Meeting

At minimum, the Customer and SkyHawk will meet twice annually; in October to prepare for the upcoming winter season and then again in April to prepare for summer operations. Items on the agenda will include:

- Review any major software updates to the system
- Determine if any additional system training is required

- New hardware requirements (spare parts and/or new kits)
- Requirements for Installation Service (service calls and/or new installations)
- Vehicles that require suspended service (to be discussed in the spring meeting)
- Review of any outstanding Support Tickets/Issue Log

SkyHawk Support Personnel

SkyHawk Support Team

SkyHawk's Technical Support Team works closely with the Project Management Team and Installation Technicians to offer deployment and post-sales support to our Customer base. Customers can reach the Support Desk via a toll-free support line 1-844-424-7759 ext. 2 or by sending an email to support@skyhawk.co. All issues that are emailed to support are automatically logged as a ticket in the JIRA issue-management system. Level 1 Support is the initial point of contact provided by SkyHawk. Any issues that can't be resolved by Level 1 are forwarded to the Level 2 Development Manager to assign the appropriate resource for resolution.

Level 1 Support

SkyHawk's experienced frontline Level 1 Support Team product specialists handle the lion's share of the trouble tickets on a day-to-day basis. Level 1 can assist with website and report issues, system administration, hardware configuration, installation support and hardware diagnostics/troubleshooting. All issues reported to Level 1 are logged in the Jira issue-management system and triaged based on severity outlined in our Service Level Agreements. Support resources will make every effort to resolve the issue as quickly as possible. Issues that can't be resolved by Level 1 Support are escalated to Level 2 Support.

Level 2 Support

Level 2 support is comprised of a team of highly skilled software developers and hardware engineers located in SkyHawk's head office in St. John's, NL. Level 2 support will evaluate the issue and advise the SkyHawk Project Manager/Account Manager of the expected resolve date, who will communicate back to the Customer's Project Manager, and/or the person who raised the ticket. Issues that are considered low risk may be implemented into the production environment as "Hot Fixes", while fixes that require more development effort and testing are scheduled for implementation into a regularly scheduled maintenance release, which typically takes place once per month.

SkyHawk Support Team			
Team Member	Project Position	Phone	Email
Support Team – Level 1	Product Support Specialists	1-844-424-7759 x2	support@skyhawk.co
Krista Schmidt	Director of Operations	289-270-0899	Krista.schmidt@skyhawk.co
Mark Callahan	Subject Matter Expert – Software – Level 2	709-737-2583 x27	mark.callahan@skyhawk.co
Derrick Dunne	Subject Matter Expert – Hardware – Level 2	709-737-2583 x32	derrick@skyhawk.co
Sean Hogan	Subject Matter Expert – System Architect - Level 2	709-737-2583 x31	sean@skyhawk.co

The SkyHawk Support Team is available 8:30 am – 5:00 pm, Monday through Friday for email and Telephone support. Emails are not monitored outside of business hours however Telephone support is available 24/7/365 for Critical Issues classified as Priority 1 or Severity 1.

After Hours Response for Critical Issues

Any issues called into the Technical Support Line outside of SkyHawk business hours are automatically forwarded to Telelink call centre that operates 24/7/365. Any issues that can't be resolved by Telelink and are determined to be critical in nature are escalated to the appropriate personnel via the emergency call out procedure. Examples of critical issues are website down/users cannot log in, or the system is up but the vehicles are not updating with live data. SkyHawk will take appropriate actions and pull together the resources necessary to resolve critical issues as quickly as possible. Any non-critical issues are deferred to the SkyHawk level 1 support team to address the next business day.

Account Manager

After project implementation is complete, the Account Manager will take on the role of the Customer's main point of contact for any issues besides regular ongoing support. The Account Manager is responsible for ensuring the Customer is kept up to date on the software development roadmap and new hardware technologies. The Account Manager is also responsible for providing quotes when reordering hardware or sourcing new products, establishing regular meeting intervals and coordinating training as required.

3 - Description of turnkey system planning, coordination and process:

a. Pre-installation coordination

At SkyHawk, careful planning and collaboration with the client will ensure a successful "Go Live". As part of the planning process, we establish clear benchmarks by which a project team can measure progress. These benchmarks make it clear where a project stands and allows adjustments to be made in the event changes are required.

The Go-Live Assessment and Plan is intended to aid the project and stakeholders in planning for the AVL installation, testing and roll-out. It can be used to plan the go-live event and to identify any issues that need to be addressed beforehand. The checklist will help eliminate some of the "unknowns" that often occur on the first day of system implementation.

Go-Live planning includes, but not limited to:

- Set the Go-Live date with the client
- Use the Go-Live date to plan all aspects of 50 Proof of Concept vehicles, UAT and roll-out completion and to allow for contingencies.
- Determine the rollout strategy; installation of 50 Proof of Concept vehicles, priority winter vehicles and all remaining vehicles to be outfitted with the AVL equipment.
- Communications to key individuals such as, project team members, stakeholders, yard superintendents, of go-live date when it appears certain and request their support during the installation
- Review goals and objectives with key stakeholders and reaffirm. Make any necessary changes as required in order to accomplish the client's goals and objectives.

The following is a sample Go-Live Assessment and Plan for the client's AVL project:

Task	Status	Comments
Contract Award	Completed	Communication
Project Managers Appointed	Completed	Communication
Kick-Off	Scheduled	
Requirements Capture	In Progress	
Delivered Project Management Documentation	In Progress / On-Going	

Hardware Delivered	In Progress	
Delivery of ConnectAnywhere Training for End Users	In Progress	
Delivery of AVL Hardware Installation to client Technicians	In Progress	
Proof of Concept 50 Vehicles - UAT Pass	In Progress	General Comm. of UAT Pass
Systems Validation & User Acceptance Test Ends	In Progress	
Prioritized Winter Vehicles - UAT Pass	In Progress	General Comm. of UAT Pass
Systems Validation & User Acceptance Test Ends	In Progress	
Remaining AVL Equipment Installed	Not Started	
Systems Validation & User Acceptance Test Ends	In Progress	
Transition to Operational Support	Not Started	
Meeting - ~1 Week to Go-Live	Not Started	Communication of Status
Meeting - ~3 Days to Go-Live	Not Started	Communication of Status
Meeting - Go-Live Day	Not Started	General Comm. of Status Go-Live
Post Go-Live Stabilization Period	Not Started	
Lessons Learned Captured	Not Started	
Close	Not Started	

b. Project coordination

SkyHawk's Project Team utilizes the Project Management Institutes (PMI) project methodology phased approach that is broken down into five (5) process groups: Initiate, Plan, Execute, Monitor and Close. In each process area we have identified key documents and tools to serve as inputs which result in deliverables for each phase.

SkyHawk's project team will spend a considerable amount of effort on detailed requirements gathering to ensure a complete understanding of the client's needs and will compile a comprehensive Project Plan which we feel is critical to the project success. The Project Plan will be updated regularly as the project progresses, and will establish project roles and responsibilities, detailed schedule of tasks, Quality Plan, risks, and Change Control. Additionally, SkyHawk's project team will work with the client's project team in preparing a full updated project schedule, including the client's installation schedule. Bi-weekly status meetings will be held to review the project schedule and to review any open issues in SkyHawk's JIRA ticketing system.

Project Communication: Project Communication will be established in the form of a regularly scheduled project meetings with status reports issued weekly. The status report will contain at a minimum the following information:

- Dashboard view on the progress of installations, tracking completed installs to planned
- Task/Action Item List from previous meetings
- Defect/Issue Log generated from the Jira Ticketing System

In addition, SkyHawk will collaborate with the client on preparing awareness communications for ConnectAnywhere training, hardware installation training, etc. as appropriate.

Communication Plan: The Project Communication plan will be created in partnership with SkyHawk and the client's Project Managers to outline how the AVL project team will be communicated during the project.

The Communication Plan shall be completed early enough in the project to be included for review at the Project Kick-off Meeting. Communications include but not limited to status, meetings, issues, deliverables access, and design/ document reviews.

Below is a sample Communication Plan:

What	Who / Target	Purpose	When / Frequency	Type / Method	Date Complete
Discovery Meeting	All stakeholders	Identify all stakeholders and provide a forum for all project team members to discuss schedule, scope, team, communications, and other items	As many as required at the start of the Project Initiation phase - 60-90 minutes session(s)	Meeting - In person / Virtual	
Project Kick-off Meeting	All stakeholders	Familiarize the project team and stakeholders with the project, review the project charter and receive buy-in from all project participants. Future meeting schedules will be defined and discussed, and meeting minutes will be documented.	At the end of the Project Initiation phase. - 60-90 minutes	Meeting - In person	
Awareness Communication: General information of AVL Project	TBD	Communicate general information to Stakeholders about coming changes	Two months before implementation. Two weeks update about changes. Two days before implementation	Email to appropriate stakeholders using the client's communication process	
Team Status Meeting	Entire Project Team	Review Project Register: Tasks, Schedule, Assignments, RAID Log, Change Requests, Open Tickets	Regularly Scheduled. Weekly/Bi-Weekly (30-60 minutes)	Meeting - In person / Virtual Meeting with standardized agenda and minutes.	
Sponsor Meetings	Sponsor(s) and Project Manager	Update Sponsor(s) on status and discuss critical issues. Seek approval for changes to Project Plan.	Monthly and/or as needed when issues cannot be resolved, or changes need to be made to Project Plan - 30-60 minutes	Meeting.	

Training Awareness Communication to ConnectAnywhere Users	Users of the application	Inform users of the changes to the existing application	Two weeks before implementation. Two days before implementation	Training: TBD Targeted email communication to system users	
Periodic Demos and Targeted Presentations	Specific Groups and/or End Users	To gain input from specific groups and keep end users apprised of features	As needed to demonstrate functionality and receive feedback in a timely manner - 30-60 minutes, as required	Meeting - In person / Virtual Presentation and Discussion	
FAQ	Users of application	Document and communicate Frequently Asked Questions about the application captured from various inputs	As needed.	Email	
Project Closing Meeting	Project Manager, Project team, key stakeholders, and sponsor(s)	Conducting the post project review meeting will allow the project team and the client's project participants stakeholders to gather one last time to ensure that there are no outstanding issues or work. This will also provide a forum to review lessons learned throughout the project.	End of project or end of major phase - 60-90 minutes	Meeting - In person / Virtual Standardized agenda and minutes.	
Other...	TBD by the team.	General communications.	As needed.	TBD	

Reporting Methods: During project implementation, the Status Report will be issued bi-weekly, prior to the Project Team Meeting. The Status Report will contain percentage complete and dashboard views of scope, schedule, cost, and quality. It will be prepared in formats approved by the client's, and will contain at a minimum the following information:

1. Progress Dashboard showing percentage complete from previous meetings.
2. Defect Log generated from the Jira Ticketing System.
3. Project Status as it relates to the Work Plan.
4. Deliverables status.
5. Planned activities for the upcoming two (2) week period.
6. Future activities.
7. Requirements Traceability Matrix (RTM)
8. Report and remedies in case of falling behind Schedule.
9. User Acceptance Test Feedback
10. Risk/Action/Issues/Decision (RAID) Register

c. Installation and Testing process

All SkyHawk's products are highly tested to ensure optimal quality. A description of the processes is as follows:

Our software development team uses an Agile product development methodology. Agile development is a group of software development methods in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, and continuous improvement, to encourage rapid and flexible response to change. A key feature of the Agile methodology includes early and frequent releases of new products, in small but fully functional increments. This promotes early customer engagement and feedback, which guides the continued development of a feature into its final form. Sales, project management, and development staff are all key contributors to the process. Clients may also be directly engaged in the process or may be represented by the sales or project management staff.

SkyHawk has established methodology and procedures for Quality Assurance and Control for hardware and software validation through a variety of test methods, checklists, and test plans, change control, and corrective action plans. Everyone is responsible for delivering quality work in their respective area. For a full description of SkyHawk's testing procedure, please refer to our Installation Plan.

SkyHawk manages software configuration through Subversion, in combination with a commercial issue-management system called JIRA that records all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration).

SkyHawk employs JIRA to record all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration). The workflows established in JIRA are integrated with the Company's Agile software development process.

We schedule maintenance releases each month, if warranted. New feature releases are incorporated into this schedule as required, with initial deployment on a test system for internal validation. In addition, Priority 1 or Severity 1 defects are addressed in real time with a fix or patch applied to the affected system(s) as soon as they are available and tested. Priority 1 defects are defined as issues which have rendered a system feature inoperable, without a workaround. Severity 1 defects are defined as issues which have not occurred but which, if triggered, would result in an impact like a Priority 1 defect.

SkyHawk Telematics applies a Lean Process philosophy to all aspects of its day to day operations, including software development, which supports increased productivity, competitiveness, and continuous improvement, while empowering our employees to problem-solve and strive for organizational excellence. Our Software Development Group adheres to well-defined processes to ensure that its services are provided in a focused manner. Under this methodology, requirements are clearly defined, progress against goals can be measured, and reliable software is produced.

All defects found during User Acceptance Testing must be reported to SkyHawk Project Manager for entry into the Jira ticketing system. The Project Manager will record the details of the defect under the Issue Type "Bug" and include the following information:

- Date/Time the defect was created
- Who reported the defect?
- Brief Summary of the defect
- Detailed defect Description including steps to reproduce the defect
- Software or hardware component(s) affected
- Any associated documents are added to the Jira ticket as Attachments ie: Test Plan, Test Results, screenshot(s) of defect

After the defect information is captured, the ticket will be triaged by the Support Desk, assigned a Severity Level, and then the ticket is assigned to the resource(s) best fit to resolve the issue. All defects logged into Jira are exportable into a Defect Log Report in either MS Excel or PDF format.

d. Client Infrastructure and support assessment process

SECURE DESIGN

SITE SELECTION: Prior to choosing a location, AWS performs initial environmental and geographic assessments. Datacenter locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another.

REDUNDANCY: Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY: AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Using Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

CAPACITY PLANNING: AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

BUSINESS CONTINUITY & DISASTER RECOVERY

BUSINESS CONTINUITY PLAN: The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

PANDEMIC RESPONSE: AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

MONITORING & LOGGING

DATA CENTER ACCESS REVIEW: Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or

contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

DATA CENTER ACCESS LOGS: Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

DATA CENTER ACCESS MONITORING: We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV: Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS: Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION: Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require everyone to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

DEVICE MANAGEMENT

ASSET MANAGEMENT: AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

MEDIA DESTRUCTION: Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

OPERATIONAL SUPPORT SYSTEMS

POWER: Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

CLIMATE AND TEMPERATURE: AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION: AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION: In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

EQUIPMENT MAINTENANCE: AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

ENVIRONMENT MANAGEMENT: AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

ONGOING DATA CENTER RISK MANAGEMENT: The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business. This process also takes regional regulatory and environmental risks into consideration.

THIRD-PARTY SECURITY ATTESTATION: Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

e. End user Acceptance process

SkyHawk Telematics has extensive hardware validation testing and full system user acceptance testing that the project management team conducts during and after installations. SkyHawk will collaborate with the client to perform system testing and validation. The Project Manager will provide standard test plan templates and will assist the client with User Acceptance Testing. Training will be provided to the client's staff on how to properly test and validate software and hardware. The client's staff are encouraged to participate in all areas of system testing as we feel it provides them with a greater understanding of the system and leads to earlier adoption.

The SkyHawk Support team will provide technical support during the testing process. Over-the-air updates and configuration can be sent by the support team, as well as assisting the technicians with onsite programming. The client's personnel shall be present at all installation locations to observe all testing procedures performed. The testing team will be provided full training documentation, including the ConnectAnywhere™ system user guide, hardware information and troubleshooting guides.

The following is an outline of testing to be performed by the Project Team:

Testing Strategy: SkyHawk will use live real-time data and historical data from the time of vehicle installation to validate the information provided in the system is correct. All testing will be performed on the City's SkyHawk ConnectAnywhere system with SkyHawk helping to facilitate the list of tests established.

Test Procedures: SkyHawk personnel will assist the City through the detailed list of tests established in the Test Procedure document

Demonstration: Through a detailed list of step by step process, SkyHawk will demonstrate to the City the functionality of the different features that were requested. This includes vehicle input status, real-time notification, and data accuracy.

System Validation Testing: This testing is performed by SkyHawk to validate the ConnectAnywhere website is set up per the client's requirements and the website is functioning as expected. This test is typically completed one week prior to installations. All mapping functions and menu items are tested for expected behaviour and to ensure of customer-specific requirements are available on the website. Phase 2 is conducted in the early stages of installation, usually, on the first or second day after some vehicle installations are complete and, real-time data is available for the testing. This testing will include data accuracy drive tests, real-time alerts, and report data validation.

Hardware Validation Testing: This testing is performed by the Installation Technician on each vehicle is the final stage in the installation process, it ensures that the hardware is installed correctly, and the modem has been updated with the correct configuration. This test includes verification of GPS message data, ignition on/off, idle verification, integration validation, input status, and power shutdown.

Calculation: Determine the run time calculations, amount of material used, average spread rates and verify the reports represent the calculated values.

User Acceptance Testing (UAT): SkyHawk will work collaboratively with the clients to perform User Acceptance Testing on the selected vehicles. First, the selected vehicle(s) must complete the prerequisite Hardware Validation Testing. Next, the basic system functionality will be verified on the website in addition to a drive-test to verify real-time alerts and validate data collected in the reports such as spread rate of salt, liquid rates, the total amount disbursed, geofenced area and plow up/down. The steps to perform this test will be recorded in the approved UAT test plan. The Client will record comments from the test process and indicate Pass or Fail. Any items with a fail will be recorded in the Jira ticketing system to track issue resolution.

Analysis: Verification of vehicle test runs where actuals are recorded and compared to the output on the system reports.

Test Management: System Validation, Hardware validation, Calibration testing, IAT and Commissioning Test will be conducted by the City and SkyHawk before testing is being executed by the City staff with assistance and guidance from the SkyHawk project team. Using the SkyHawk Test Procedures, the PM will record those features that were successful and those that require additional testing. For all items that require additional testing, details notes will be taken and reviewed by NHDOT. These notes will also allow SkyHawk and the City to determine which subsequent tests need to be performed to ensure all features are functioning properly.

f. Approach to maintenance and support

All SkyHawk's products are highly tested to ensure optimal quality. A description of the processes is as follows:

Our software development team uses an Agile product development methodology. Agile development is a group of software development methods in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, continuous improvement, and encourages rapid and flexible response to change. Key features of the Agile method include early and frequent releases of new products, in small fully functional units. This promotes early customer engagement and feedback which guides the continued development of a feature into its final form. Sales, project management, and development staff are all key contributors to the process. Clients may also be directly engaged in the process or be represented by the sales or project management staff.

SkyHawk has established methodology and procedures for Quality Assurance and Control for hardware and software validation through a variety of test methods, checklists, and test plans, change control and corrective action plans. Everyone is responsible for delivering quality work in their respective area. For a full description of SkyHawk's testing procedure, please refer to the Installation Plan.

SkyHawk manages software configuration through Subversion, in combination with a commercial issue-management system called JIRA that records all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration).

SkyHawk employs JIRA to record all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration). The workflows established in JIRA are integrated with the Company's Agile software development process.

We schedule maintenance releases each month if warranted. New feature releases are incorporated into this schedule as required, with initial deployment on a test system for internal validation. In addition, Priority 1 or Severity 1 defects are addressed in real-time with a fix or patch applied to the affected system(s) as soon as they are available and tested. Priority 1 defects are defined as issues that have rendered a system feature inoperable, without a workaround. Severity 1 defects are defined as issues that have not occurred but which, if triggered, would result in an impact similar to a Priority 1 defect.

SkyHawk Telematics applies a Lean Process philosophy to all aspects of its day to day operations, including software development, which supports increased productivity, competitiveness, and continuous improvement, while empowering our employees to problem-solve and strive for organizational excellence. Our Software Development Group adheres to well-defined processes to ensure that its services are provided in a focused manner. Under this methodology, requirements are clearly defined, progress against goals can be measured, and reliable software is produced.

All defects found during User Acceptance Testing must be reported to SkyHawk Project Manager for entry into the Jira ticketing system. The Project Manager will record the details of the defect under the Issue Type "Bug" and include the following information:

- Date/Time the defect was created
- Who reported the defect?
- Brief Summary of the defect
- Detailed defect Description including steps to reproduce the defect
- Software or hardware component(s) affected

Any associated documents are added to the Jira ticket as Attachments i.e.: Test Plan, Test Results, screenshot(s) of defect.

After the defect information is captured, the ticket will be triaged by the Support Desk, assigned a Severity Level and then the ticket is assigned to the resource(s) best fit to resolve the issue. All defects logged into Jira are exportable into a Defect Log Report in either MS Excel or PDF format.

(b) a description of the methods available for contacting support, days/hours (location time) that support is provided, and your after-hours support. Note: City of Burlington office hours are between 8:30am - 4:30pm local time; maintenance staff typically start at 7:00 am; and asset maintenance can occur 7/24/365.

(c) a description of your process for communicating, prioritizing, and addressing application and infrastructure problems of varying severity levels. The description should include, for different severity levels, how and how frequently the City will be updated and what information will be provided.

(g) a description of the problem tracking data that is collected, maintained and available to the City either online or upon request (e.g. date/time ticket open/closed, problem type, fix, reoccurrence tracking) and for how long.

SkyHawk Support Services

SkyHawk Support Team: SkyHawk's Technical Support Team works closely with the Project Management Team and Installation Technicians to offer deployment and post-sales support to our Customer base. Customers can reach the Support Desk via a toll-free support line 1-844-424-7759 ext. 2 or by sending an email to support@skyhawk.co. All issues that are emailed to support are automatically logged as a ticket in the JIRA issue management system. Level 1 Support is the initial point of contact provided by SkyHawk. Any issues that cannot be resolved by Level 1 are forwarded to the Level 2 Development Manager to assign the appropriate resource for resolution.

Level 1 Support: SkyHawk's experienced frontline Level 1 Support Team product specialists handle frontline trouble tickets on a day-to-day basis. Level 1 can assist with website and report issues, system administration, hardware configuration, installation support and hardware diagnostics/troubleshooting. All issues reported to Level 1 are logged in the Jira issue-management system and triaged based on severity outlined in our Service Level Agreements. Support resources will make every effort to resolve the issue as quickly as possible. Issues that cannot be resolved by Level 1 Support are escalated to Level 2 Support.

Level 2 Support: Level 2 support is comprised of a team of highly skilled software developers and hardware engineers located in SkyHawk's head office in St. John's, NL. Level 2 support will evaluate the issue and advise the SkyHawk Project Manager/Account Manager of the expected resolve date, who will communicate back to the Customer's Project Manager and/or the person who raised the ticket. Issues that are considered low risk may be implemented into the production environment as "Hot Fixes", while fixes that require more development effort and testing are scheduled for implementation into a regularly scheduled maintenance release, which typically takes place once per month.

The SkyHawk Support Team is available 8:30 am – 5:00 pm, Monday through Friday for email and telephone support. Emails are not monitored outside of business hours however Telephone support is available 24/7/365 for Critical Issues classified as Priority 1 or Severity 1.

After Hours Response for Critical Issues: Any issues called into the Technical Support toll-free line (1-844-424-7759 ext. 2) outside of SkyHawk business hours are automatically forwarded to Telelink call centre that operates 24/7/365. Any issues that cannot be resolved by Telelink and are determined to be critical in nature are escalated to the appropriate personnel via the emergency call out procedure. Examples of critical issues are website down/users cannot log in, or the system is up but the vehicles are not updating with live data. SkyHawk will take appropriate actions and pull together the resources necessary to resolve critical issues as quickly as possible. Any non-critical issues are deferred to the SkyHawk level 1 support team to address the next business day.

SkyHawk employs JIRA to record all requests for change, whether they are problems, feature requests or service requests (requests for change of configuration). The workflows established in JIRA are integrated with the Company's Agile software development process.

(d) a description of severity levels (including who determines the severity levels and the process to deal with disagreements), response times, and expected resolution times for each severity level, post-incident reviews and feedback surveys, and escalation processes for emergency technical support. The description should include the hours during which the Proponent will work to resolve issues (by severity level if the hours vary according to severity level).

SkyHawk has three levels of technical support to resolve issues reported by its clients. Level 1 Support is the initial point of contact provided by the SkyHawk Support Team. Any Issues that can't be resolved by Level 1 are forwarded to the Technical Operations Manager to assign a Level 2 resource for resolution. Our frontline Support Desk technicians handle the lion's share of our trouble tickets on a day-to-day basis. Escalation to Level 3 status will involve our software/hardware engineers or field technicians. For problems that require escalation due to urgent nature or unsatisfactory response, the issue can be assigned to our project and company management.

The Help Desk is available 24 hours each day, 365 days per year, for reporting of issues and resolution of simple requests: North America: Toll-free number 1-844-424-7SKY (1-844-424-7759) extension #2 or at support@skyhawk.co.

Minor Issue - SkyHawk shall respond within 1 business day - At the discretion of SkyHawk, will provide a Workaround and/or Error Correction in the next Version, Upgrade, or Update.

Serious - SkyHawk shall respond the same business day, or if outside SkyHawk business hours, the next business day. - SkyHawk shall provide a Patch within 5 business days following response if possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.

Critical - SkyHawk shall respond the same business day, or if outside SkyHawk business hours, will attempt to respond ASAP, but in all cases within 1 hour the next business day. - SkyHawk shall provide a Patch as soon as possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.

(e) a description of the process by which requests for support can be escalated.

(f) a description of troubleshooting and error tracking methods (e.g. WebEx, Skype for Business, GoToMeeting, remote desktop, system monitoring).

SkyHawk has three levels of technical support to resolve issues reported by its clients. Level 1 Support is the initial point of contact provided by the SkyHawk Support Team. Any issues that cannot be resolved by Level 1 are forwarded to the Technical Operations Manager to assign a Level 2 resource for resolution. Our frontline Support Desk technicians handle the lion's share of our trouble tickets on a day-to-day basis. Escalation to Level 3 status will involve our software/hardware engineers or field technicians. For problems that require escalation due to urgent nature or unsatisfactory response, the issue can be assigned to our project and company management.

A client may request a report of their open/closed issues at any time from our support team. In addition to reporting issues through the Support Desk, the assigned Project Manager or Account Manager, the Customer may follow this escalation path noted below if a reported problem is not resolved within the expected timeframes or not resolved to their satisfaction:

	Name	Title	Phone	Email
1	Krista Schmidt	Director, Operations	289-270-0899	Krista.schmidt@skyhawk.co
2	Mark Gillingham	Vice President	709-737-2583 x34	mark.gillingham@skyhawk.co
3	Paul Anderson	President	709-737-2583 x24	paul.anderson@skyhawk.co

(h) a description of the warranty for implementation and configuration services, any limitations on the warranty and any limitations on the remedies. The desired warranty is in four parts, one for each phase, the warranty for each phase being for a year triggered by the completion of the phase. Each warranty is for the services provided in the phase.

(j) a description of your Service Level Agreement for cloud solutions including the methodology for granting service level credits and the amount of risk individually and in the aggregate.

Equipment warranty and all service warranty information for the proposed solution.

We warrant that SkyHawk Telematics-Branded Products and all other products and services rented, sold or resold will be free from defects in materials and workmanship for a period of one (1) year from the date of delivery with respect to hardware and will materially conform to their published specifications for a period of one (1) year with respect to software and software-based services.

A sample contract including SkyHawk's End User License Agreement and Warranty policies is attached. SkyHawk offers an Extended Warranty, the cost is 10% of equipment cost per year of the extended warranty period.

- Extended warranty period must be accepted and agreed upon before the end of the manufacturer's warranty.
- Payment for the extended warranty term is due annually based on the client agreeing to the warranty renewal.
- Shipping fees to the SkyHawk office in Oakville, ON are the responsibility of the client. SkyHawk will cover the return shipping fees.
- Costs to remove and re-install equipment covered by warranty are not included in the warranty fee.

(i) if software customization impacts support services how it does so.

The Service Level Agreement for time to resolve issues applies to the production environment only. Issues found when testing customized software will be resolved using best efforts to keep the project schedule, but standard Service Level Agreements do not apply.

(k) a description of any incidents or events that are not included as part of support and any limitations of the Proponent's performance of support including any software currency requirements; and

(l) a description of the anticipated requirements for City staff to support the application and infrastructure (the infrastructure indicated in response to submission requirement 3) directly and what roles are required, and any assistance required from the City in order for you to provide your support services. Include in the description the number (and/or fractions) and types or category of full-time City staff anticipated to be required for this support.

After the project implementation is complete, it is recommended the City to appoint an AVL Coordinator to liaise with the SkyHawk Account Manager. A key responsibility of the AVL coordinator is approve changes in the system such as authorize a new user access or decide who shall have access to a new report offering. A monthly meeting is recommended to review any open issues, be kept abreast of any upcoming changes to the SkyHawk system and determine ongoing needs for training or new equipment installations.

For SkyHawk to support service calls, we must be provided a contact who can arrange for the vehicle to be made available during the service call. Depending on the vehicle type, a vehicle Operator may be required to assist the installation technician with the vehicle testing i.e.: operate the snowplow.

g. Initial and Ongoing Training provided

Training will be provided based on the client's end-user requirements workshop, the personnel's job responsibilities, their interaction with ConnectAnywhere and the various system components. SkyHawk has a comprehensive training team that

will provide on-site and / or webinar training as per requirements of the client and will provide full product training for the full group of administrator users. Additionally, SkyHawk will provide web-based remote training on a quarterly basis to all system users to familiarize them with the usage and functionality of the ConnectAnywhere monitoring website. These sessions are intended to reinforce initial training.

SkyHawk will provide the comprehensive set of training materials in both digital and hard copy for all aspects of the ConnectAnywhere system. In-person and/or Webinar training delivery formats are available to the identified end-users of the client.

The training covers all aspects of the system, including:

- ConnectAnywhere Software for Basic End Users
- ConnectAnywhere Software for System Administrators
- Equipment Installation, Diagnostics, Service & Repair

ConnectAnywhere High Level Topics for Basic End-User Training: A full Software tutorial for the end users of the ConnectAnywhere web-based monitoring solution, including but not limited to:

- Log-in and out of Account
- Mapping interface features, including configuration for polygons
- Reporting capabilities
- Geofence creation
- Asset Status features

ConnectAnywhere High Level Topics for System Administrator End-User Training: A full Software tutorial for the System Administrators of the ConnectAnywhere web-based monitoring solution, including but not limited to:

- Creating assets and hardware records
- User logins/account profiles
- Hardware swap procedure
- Decommissioning vehicle procedure

ConnectAnywhere Re-training and Technical Support: Webinars on new features

- Refresher training as needed
- Assistance provided by Support Team
- Support Contract info/hours

In order to satisfy the client's requirement to train end users; SkyHawk's Training Program will be divided into three (3) modules and delivered at various locations as agreed upon with the client. These modules can be modified and tailored to the client's requirements.

ConnectAnywhere Module(s)

Audience	ConnectAnywhere Module(s)	Estimated Duration*
Basic User Overview	Overview of SkyHawk Telematics and interactive/live demonstration of using various functions of the system, such as but not limited to: • Hardware installed and high-level features • Landing Page and Login • Overview of Menu Tabs and Panes • Map View and User Interface • Vehicle Location • History Report and its data	~60 minutes

	• Geofences • Help, User Guides and Release Notes • Question and Answers	
Reporting Overview	Pre-requisite Training Basic User Training Focused training for end users who will be using the system to run reports, such as but not limited to: • Vehicle Trip Report • Speed Report • Winter Operations Trip • Winter – Material by Time • Spreading Speeding • Utilization Report • Scheduled Reports • Help, User Guides and Release Notes • Questions and Answers • Etc.	~90 minutes
Administration Overview	Pre-requisite Training Basic User Training Reporting Overview	~60 minutes
	Focused for those end users who will be administering the system, such as but not limited to: • Admin Tab Overview and Features • Creating User Accounts and Account Templates • Asset Vehicle Folder Structure • Alerts • Linking assets • Viewing user history • Help, User Guides and Release Notes • Question and Answers • Etc.	

*Duration: Estimated time depending on the client's requirements

Onsite System Training: This deliverable provides onsite training by qualified SkyHawk Telematics staff to the Client training personnel and management for the use and administration of the system. Training will be provided based on the Client personnel job responsibilities and their interaction with ConnectAnywhere and the various system components. SkyHawk's software training specialist will provide on-site training and will provide full product training as well as training printouts for participants for the full group of admin users in conjunction with installation.

The training solution includes the provision of all required digital and print materials. SkyHawk will provide the comprehensive set of training manuals in both digital and hard copy for the Operation, Diagnostics and Service & Repair for all aspects of the system.

Below is a high-level training topic list that will include the following topics and can be tailored to the Client requirements:

- A full Software tutorial for the End Users of the ConnectAnywhere web-based monitoring solution, including but not limited to:
- Log-in & out of Account
- Mapping interface features, including configuration for polygons
- Reporting capabilities
- Geofence creation

- Asset Status features
- A full Software tutorial for the System Administrators of the ConnectAnywhere web-based monitoring solution, including but not limited to:
- Creating assets and hardware records
- User logins/account profiles
- Hardware swap procedure
- Decommissioning vehicle procedure
- Hardware Installation & Troubleshooting training:
- Wiring and wire routing
- Hardware component installation and configuration
- Hardware commissioning and test
- Diagnostic and troubleshooting procedures
- Retraining and Technical Support
- Webinars on new features
- Refresher training as needed
- Assistance provided by Support Team
- Support Contract info/hours

Hardware Install & Troubleshooting Training: Hardware installation and troubleshooting training will be conducted on-site to cover operations, diagnostics, installation, service, and repair, as per requirements. The SkyHawk installation approach encourages including the client's in the installation process to allow a hands-on training approach and to reduce the Client overall operational costs.

Equipment Installation, Diagnostics, Service & Repair: SkyHawk, will provide hardware installation and hardware troubleshooting/diagnostics training to the client's assigned fleet services team members. SkyHawk will offer a full installation certification training program to the Client Fleet Services dedicated staff. SkyHawk recommends that installation and troubleshooting training be conducted at the start of installations for Client mechanical staff to get a hands-on learning experience. The installation training will include hardware wiring and wire- routing, as well as hardware commissioning and testing procedures. Installation and hardware troubleshooting documentation will also be provided for reference.

Product Training: Our training programs are designed to ensure all user groups of the SkyHawk Telematics offerings obtain maximum value from the user experience. Programs include on-site & remote web-based training utilizing a variety of methods including software, videos & printed resources.

Prerequisite/Basic Knowledge Concepts (Mechanic Installation Training): The following are, but not limited to, basic prerequisite and basic knowledge requirements of the client's mechanics and installers. Mechanics should already be familiar with:

- Shop Safety and First Aid
- Fire Safety
- Vehicle Safety (especially working under the hood, moving vehicles)
- Knowledge and use of appropriate PPE (personal protective Equipment)
- Basic Electrical knowledge - voltage, current, resistance, series and parallel circuits
- Use of test equipment – multimeters, continuity testers
- Continuity testing and electrical troubleshooting techniques
- Wire Gauge selection
- Electrical Components familiarity – resistors, fuses, relays
- How to make proper electrical connections (soldering techniques, crimps)

The client's Mechanics/Installers should have an awareness of the following, but not limited to, the following vehicle concepts (SkyHawk can also aid/coaching):

- Vehicle battery familiarity, safe operating procedures, and testing
- ECM port identification and differences (OBD2, J1939, J1708)
- Fuse panels and fuse identification
- 12 and 24-volt vehicle systems, frame grounds
- Wire pulling techniques
- Exposed wire protection (shrink tubing application, electrical tape application)
- Antenna placement (cellular/GPS and satellite)
- Quality installation techniques:
- Proper wire routing/placement (raceways, panels, floorboard access)
- Split loom usage
- Tie wraps
- Surface cleaning for adhesive installation

Re-training: As part of the training package, SkyHawk provides the client with comprehensive training materials allowing personnel and management to refer to the tutorials at any time by simply clicking a link. The tutorial package consists of screen-flow diagrams with text, to allow users to select their preferred learning program. The sales and technical teams at SkyHawk are very active in participating in and attending relevant technical and AVL events to ensure that we offer cutting-edge, competitive technologies. SkyHawk will provide training on any major software features changes, via webinar sessions at no additional cost for the duration of the contract.

- The following documents will be provided to assist with training:
- Installation manuals
- Hardware Diagnostics & Repair manual
- System Operation manuals

Web-based System Training: In addition to initial onsite training, SkyHawk also recommends the Client participate in a follow-up webinar training session 2-3 week following installations when the system has the newly installed vehicles set up and is fully functional. This training consists of web-based remote training to all system users to familiarize them with the usage and functionality of the ConnectAnywhere monitoring website. These sessions are intended to reinforce initial training. Each session can support up to 50 online trainees.

Post-implementation, software, diagnostics, install, service and repair training will be conducted twice per year by SkyHawk training staff and is recommended to be done once in the fall before winter activities, and again at the end of the winter season. Further, SkyHawk will also provide webinar training on a quarterly basis to unlimited users, to refresh, train new employees and cover any major software feature enhancements/changes.

Training Documentation: As part of the training package, SkyHawk offers a comprehensive software training guide, allowing the Company's personnel and management to reference any feature within the system. SkyHawk will provide the client with training on any major software features changes, via webinar sessions at no additional cost for the duration of the contract.

Hardware Documentation: All documentation required for understanding the hardware, installing, troubleshooting, and for performing repairs shall be provided to the client by SkyHawk.

Training and Workshop Schedule/Timelines: SkyHawk shall collaborate with the client to produce a reasonable schedule and accommodate the training.

h. On-going support and enhancement over the life of the agreement

The transition from project implementation to Operational Support (post go-live) is part of the Project Closing phase of a project. All in-scope AVL devices and in-scope peripherals have been installed, tested, and are successfully reporting in ConnectAnywhere. The system has completed the UAT and operating as expected. Once the last installation is completed, the Project Manager will send a communication to the City that the project is now entering the Closed phase and will be

transferred to the assigned Account Manager and Operational Support. They are responsible for the following ongoing support items:

Account Manager:

- Schedule additional ConnectAnywhere user training and coaching
- Share new hardware/software features and functionality
- Ordering of hardware
- Request changes to data plans
- Billing inquiries
- General inquiries
- Escalation of unresolved issues to the management team

SkyHawk Support Desk:

- Technical support and troubleshooting
- Installation support and testing
- Dispatch service call visits
- ConnectAnywhere user support (password reset, account adjustments, etc.)
- General inquiries

For ongoing support, the SkyHawk Support Desk will assist the Customer with troubleshooting malfunctioning hardware devices. If the device can't be fixed through Over the Air (OTA) configuration changes, manual reprogramming or additional diagnostic measures, the SkyHawk Support Desk will recommend either returning the device to SkyHawk for repair or dispatch a field technician for a service call.

The Customer shall contact SkyHawk Support Desk when making the following configuration changes:

- Baseline odometer or engine hour value
- ECM type
- Change to vehicle voltage of ATrack device
- Change to installation method of ATrack device (3-wire, hardware ignition only, or ECM power)

Installation, Removal or Repair of Hardware: The Customer shall contact the SkyHawk Project Manager or SkyHawk Support Desk to schedule a service call if a unit is to be removed, installed, or needs repair. SkyHawk will dispatch a trained, qualified service technician to the Customer site. SkyHawk technicians are equipped with a small stock of commonly used spare parts so they may complete a repair during the same service call as the initial troubleshooting. Equipping our Service Technician with spare parts results in both time and cost savings for the Customer.

Re-Order of Hardware: The Customer shall contact their SkyHawk Account Manager to place an order for hardware. A quote will be provided for the Customer's review and approval. A P.O. is required from the Customer to authorize the purchase.

Return Material Authorization (RMA): The Customer shall contact the SkyHawk Support Desk to obtain authorization before returning any defective or un-used hardware. The SkyHawk Support Desk will respond in writing with the RMA number, return address and instructions for preparing the courier documents.

Discontinued Hardware: When a hardware device is to be discontinued, the SkyHawk Account Manager will notify the Customer in writing of the discontinued product and will provide as much advance notice as possible. A suitable replacement will be recommended by the Account Manager with an accompanying price quote. The SkyHawk Support Desk will provide an installation guide and assistance to install the new device for a demo period or can arrange for a service call to have the new device installed by the SkyHawk approved installation sub-contractor.

Communication

Regularly Scheduled Software Release and Maintenance Update: The SkyHawk Support Desk will notify key personnel of the Customer via email five (5) business days in advance of an upcoming Software Release and Maintenance Update. The first notice will include the date/time and approximate duration of the maintenance window. A reminder email is sent the day of the update and this notice will include the release notes. Once the update is complete, the release notes can also be found on ConnectAnywhere under the Help menu.

Service Interruption or Unplanned Outage: The SkyHawk Support Desk will notify key personnel of the Customer via email as soon as possible when any service interruption or unplanned outage of the software is detected. The Support Desk will continue to provide regular updates via email until the issue is resolved.

Annual Meeting: At a minimum, the Customer and SkyHawk will meet twice annually; in October to prepare for the upcoming winter season and then again in April to prepare for summer operations. Items on the agenda will include:

- Review any major software updates to the system
- Determine if any additional system training is required
- New hardware requirements (spare parts and/or new kits)
- Requirements for Installation Service (service calls and/or new installations)
- Vehicles that require suspended service (to be discussed in the spring meeting)
- Review of any outstanding Support Tickets/Issue Log

SkyHawk Support Personnel

SkyHawk Support Team: SkyHawk's Technical Support Team works closely with the Project Management Team and Installation Technicians to offer deployment and post-sales support to our Customer base. Customers can reach the Support Desk via a toll-free support line 1-844-424-7759 ext. 2 or by sending an email to support@skyhawk.co. All issues that are emailed to support are automatically logged as a ticket in the JIRA issue management system. Level 1 Support is the initial point of contact provided by SkyHawk. Any issues that can't be resolved by Level 1 are forwarded to the Level 2 Development Manager to assign the appropriate resource for resolution.

Level 1 Support: SkyHawk's experienced frontline Level 1 Support Team product specialists handle the lion's share of the trouble tickets on a day-to-day basis. Level 1 can assist with website and report issues, system administration, hardware configuration, installation support and hardware diagnostics/troubleshooting. All issues reported to Level 1 are logged in the Jira issue-management system and triaged based on severity outlined in our Service Level Agreements. Support resources will make every effort to resolve the issue as quickly as possible. Issues that can't be resolved by Level 1 Support are escalated to Level 2 Support.

Level 2 Support: Is comprised of a team of highly skilled software developers and hardware engineers located in SkyHawk's head office in St. John's, NL. Level 2 support will evaluate the issue and advise the SkyHawk Project Manager/Account Manager of the expected resolve date, who will communicate back to the Customer's Project Manager and/or the person who raised the ticket. Issues that are considered low risk may be implemented into the production environment as "Hot Fixes", while fixes that require more development effort and testing are scheduled for implementation into a regularly scheduled maintenance release, which typically takes place once per month.

The SkyHawk Support Team is available 8:30 am – 5:00 pm, Monday through Friday for email and telephone support. Emails are not monitored outside of business hours however Telephone support is available 24/7/365 for Critical Issues classified as Priority 1 or Severity 1.

After Hours Response for Critical Issues: Any issues called into the Technical Support Line outside of SkyHawk business hours are automatically forwarded to the Telelink call centre that operates 24/7/365. Any issues that cannot be resolved by Telelink and are determined to be critical in nature are escalated to the appropriate personnel via the emergency call-out procedure. Examples of critical issues are website down/users cannot log in, or the system is up but the vehicles are not updating with live data. SkyHawk will take appropriate actions and pull together the resources necessary to resolve critical

issues as quickly as possible. Any non-critical issues are deferred to the SkyHawk level 1 support team to address the next business day.

Account Manager: After the project implementation is complete, the Account Manager will take on the role of the Customer's main point of contact for any issues besides regular ongoing support. The Account Manager is responsible for ensuring the Customer is kept up to date on the software development roadmap and new hardware technologies. The Account Manager is also responsible for providing quotes when reordering hardware or sourcing new products, establishing regular meeting intervals, and coordinating training as required.

4 - Service Factors:

SkyHawk Telematics has been delivering advanced telematics solutions to government mixed fleet, including winter operations functionality, for more than 10 years, to clients in the USA and Canada.

The SkyHawk System, ConnectAnywhere, is a web-based monitoring solution designed for enterprise level, cloud-based service which facilitates the real-time visibility and management of an organization's valuable assets. The service provides unique asset identification, GPS location and vehicle status integration with sensory information such as PTO, beacon, and brooms.

As the name implies, users of the ConnectAnywhere system only require an internet connected computer or mobile device with a supported web browser to access information most anywhere in the World.

SkyHawk's ConnectAnywhere web-based monitoring solution is hosted out of AWS Data Centre guarantees 99.9% service availability, 24/7 onsite support, automated system monitoring and dynamic resource allocation controls. For instance, as more network bandwidth, CPU, RAM, storage is required, the system dedicates the necessary computing resources. Furthermore, the solution provides a separate dedicated database, virtual server, IP address and SSL security. These dedicated resources ensure the highest level of performance and that the system is not degraded by other companies sharing the same system resources.

ConnectAnywhere allows unlimited user accounts or logins with Skyhawk staff providing the initial account setup and administration. Once the system is fully operational, clients have complete administrative IT access to the features and functionality of the system. The ConnectAnywhere solution provides complete GIS mapping integration and interface capabilities to other client software applications with REST API.

Some key features of the SkyHawk solution include:

- The ability to obtain ECM engine data including fuel efficiency characteristics such as: Total Fuel Used (L),
- Fuel Rate (L/h), Instantaneous Fuel Economy (km/L), Average Fuel Economy (km/L) when available from the vehicle manufacturer.
- The ability to report on unsafe driver actions such as speeding (with local speed zone), harsh braking, harsh acceleration, etc.
- Alerts and alarms that are configurable and which can be delivered directly to users via email or SMS messaging
- Unlimited number of user accounts (usernames and passwords) with complete administrator level access and system control, multiple user access levels (e.g. Viewer, Manager, Admin, etc.) controlled by administrator
- Create email and text contact lists per asset for real-time notifications
- Map options default to Google but access to client maps via ESRI/GIS link
- Website protected with industry- standard 128-bit encryption with an SSL certificate Ability to filter vehicles in real-time and the view of the data online
- Custom Geo-Fencing and alerts on activity in and out of Geo-Fenced areas Zoom-In, Zoom-Out, Pan, Drag- Zoom, Road Map Data, Air-Photo Data, etc. Access to reports in real-time online.
- Optional - Tablet support for in- cabin operations supporting advanced navigation and routing options.

- Optional - A completely integrated satellite asset tracking support for vehicles and for high valued, non-powered assets.

Our solution can integrate with other software and IT applications and is built on one of the most advanced networks and computing platforms available, providing a long-term solution to our customers. Thus, our telematics solution will meet, and in many cases exceed, all aspects and requirements of the organization.

The SkyHawk solution is provided to our clients as a monthly online service and not as "Software" in the traditional sense. Customers will not have to install any programs, routines, scripts etc. or run any software to use the SkyHawk ConnectAnywhere solution. All you need is a modern browser and an internet connection.

SkyHawk Telematics is device agnostic. We pick the best hardware manufacturers from around the globe to address each vehicle type requirements, from simple track-and-trace, to complex integrations, to vehicles with multiple IO requirements.

Each piece of hardware is selected to perfectly fit each vehicle's specific requirement and not one piece of hardware is made to fit all. Partnering with multiple hardware vendors also means that we are able to offer our clients the most current and up-to-date hardware, ensuring that we future proof your solution by not only meeting their requirements for today but being flexible to anticipate and meet future requirements.

The modems we offer have a robust set of features with reliable track records, including standard store- and-forward capabilities for when the vehicle is out of cellular coverage, as well as the ability to receive and perform over-the-air (OTA) configuration or firmware updates in the field.

This eliminates the need to physically visit the vehicle for support and maintenance.

SkyHawk's most widely used modems range from simple track and trace to the most complex of applications used for optimal winter maintenance tracking.

As an end-to-end solutions provider, with a proven track record of successful client partnerships, we understand the needs of complex deployments.

Experienced and competent subject matter experts: SkyHawk has a team that has successfully delivered similar projects of scope and scale. SkyHawk's team includes senior management/corporate project sponsors, sales account managers, project management specialists, operations/procurement/order fulfillment staff, installation teams, support staff, and financial/billing specialists.

Project Management: Effective management is vital to the overall success of any project and SkyHawk has proven its ability to deliver telematics projects to complete vehicle and feature roll with very large and complex projects.

Project Management Approach: Skyhawk's Project Team utilizes the Project Management Institutes (PMI) project methodology phased approach that is broken down into five (5) process groups: Initiate, Plan, Execute, Monitor and Close. In each process area, we have identified key documents and tools to serve as inputs that result in deliverables for each phase.

SkyHawk's project team will spend a considerable amount of effort on detailed requirements gathering to ensure a complete understanding of the Client's needs and will compile a comprehensive Project Plan which we feel is critical to the project's success. The Project Plan will be updated regularly as the project progresses, and will establish project roles and responsibilities, a detailed schedule of tasks, Quality Plan, risks, and Change Control. Additionally, SkyHawk's project team will work with the Client's project team in preparing a full updated project schedule, including the Client's installation schedule. Bi-weekly status meetings will be held to review the project schedule and to review any open issues in SkyHawk's JIRA ticketing system.

Project Communication: Project Communication will be established in the form of regularly scheduled project meetings with status reports issued weekly. The status report will contain at a minimum the following information:

1. Dashboard view on the progress of installations, tracking completed installs to planned
2. Task / Action Item List from previous meetings

3. Defect /Issue Log generated from the Jira Ticketing System
4. In addition, SkyHawk will collaborate with ODTO on preparing awareness communications for ConnectAnywhere training, hardware installation training, etc., as appropriate.

Communication Plan: The Project Communication plan will be created in partnership with SkyHawk and the client's Project Managers to outline how the AVL project team will be communicated during the project.

The Communication Plan shall be completed early enough in the project to be included for review at the Project Kick-off Meeting. Communications include but not limited to; status, meetings, issues, deliverables access, and design/document reviews.

Reporting Methods: SkyHawk, in collaboration with our client's project team, shall determine reporting and communication cadences. During the project implementation phase, the Status Report will be issued weekly or bi-weekly, prior to the Project Team Meeting. The Status Report will contain percentage complete and dashboard views of scope, schedule, cost, and quality. It will be prepared in formats approved by the client and will contain at a minimum the following information:

1. Progress Dashboard showing percentage complete from previous meetings
2. Defect Log generated from the Jira Ticketing System
3. Project Status as it relates to the Work Plan
4. Deliverables status
5. Planned activities for the upcoming two (2) week period
6. Future activities
7. Requirements Traceability Matrix (RTM)
8. Report and remedies in case of falling behind Schedule
9. User Acceptance Test Feedback
10. Risk/Action/Issues/Decision (RAID) Log

Solution Configuration: SkyHawk's "ConnectAnywhere" solution is the result of our unwavering commitment to our client partners to provide them the data they require to make informed decisions to maximize operational efficiency, minimize environmental impacts, and protect the safety of both employees as well as the general public. Through continual consultations with the people responsible for the wellbeing of municipal, provincial, and state fleets and the roadways on which they operate, we have incorporated the feedback of these industry experts, along with the lessons we have learned along the way, to the data we collect and the information we report.

To accommodate the ever-increasing volume and diversity of data sources we pull from, the latest version of ConnectAnywhere is architected using modern design techniques that allow us to support many thousand simultaneous connections while maintaining flexibility through the use of the schema-less MongoDB database. This provides us the capability to add or modify the underlying data of ConnectAnywhere to support new feature development without the complexity and downtime that would be required in a more traditional relational database environment.

This flexibility also allows us to support a wide variety of data collection devices, including telematics modems, asset trackers, etc. which enable us to provide a "right-sized" solution for the highly diverse fleets our clients maintain. We also promote "configuration" over "customization"; when we are presented with a business problem to address for one of our client partners, we approach the solution in such a way to benefit all of our users, with consultations as necessary, and make the additions available to our entire client base with the capability to adjust parameters to suit their own operational needs

The client onboarding process involves our project team gaining a thorough understanding of our client's business requirements, which is then used in the setup of your ConnectAnywhere portal. Starting with the master vehicle list, we painstakingly review every vehicle and the data points to be collected from each, including such items as the ECM type, discrete inputs for PTO's, beacon lights, etc. This is then entered into ConnectAnywhere, which allows us to normalize the potentially many different sources into the consistent user experience in terms of display and reporting. From there, we can adjust the vehicle messaging profile and event thresholds to suit your business goals. We also work with you to gather the user account information to create the "account templates" that control the functionality and subset of assets that each end-user has available to them. Other key configuration items include the setup of system alerts and scheduled reports.

Specialized Solution Offering: When dealing with a complex fleet of mixed vehicles with specialized reporting functionality it is very important to acquire a solution that is designed and built for the vehicle types and operations of a large municipal organization. SkyHawk's ConnectAnywhere telematics solution has been designed and built specifically for this application and supports the specialized and advanced functionality required to operate these services more effectively and efficiently.

Installation Plan/Staff: Vehicle installations and testing are one of the most critical parts of any telematics system. At SkyHawk we refer to it as the "foundation" upon which all other functionality is built or layered. A well-designed installation plan along with a team of reliable installers is required for success. Furthermore, it has been the experience of SkyHawk that best results are achieved when a combined approach of vendor/contracted installers working in conjunction with our client's mechanics and technical staff is utilized.

Effective Communications Plan: Engagement of the client's staff and departments to obtain a deep understanding of goals and objectives, as well as obtaining input, feedback, and required "buy-in" from management, system users and stakeholders leads to a better managed and implemented solution. This is best accomplished with an effective communication and engagement plan which starts before implementation begins and carries through all project phases. SkyHawk has significant and relevant experience working with large clients in delivering successful communication plans.

Project Team: SkyHawk has assembled a team of experts in the deployment of AVL projects. They are motivated by excellence and have the combined skills and capabilities to deliver the project on time and on budget and of the highest quality.

The following is a profile of one of SkyHawk's utility clients

Fleet Composition:

Total of 10000 assets

- 5000 light duty vehicles – 50% (Sedans, Pick-up's, 4x4) – (Gas & Hybrid)
- 2000 Heavy duty trucks – 20% (Bucket trucks, 53' long hauls, Cubes)
- 3000 Utility vehicles/Equipment – 30% (VTT's, Snowmobiles, Trailers, Manlifts, etc.)

Users composition

- 1 Admin
- 50 Super Users Including management team
- 900 Users
- 200 Mechanics

Hardware Composition

- Urban areas: Atrack AX9, AX11, AS11 and AK11 for cell coverage data transmission.
- Rural areas: The above modems backed with a secondary Globalstar Smart1C modem to guarantee asset localization at all time.
- Remote areas: Skywave Orbcomm ST6100 for a full satellite experience.

Hardware Installation

- The installation process was divided between external installers and client mechanics as they have +/- 40 maintenance shops across their geographic footprint
- Skyhawk managed the external installation process.

Project Management

We implemented this project in stages and based on priority. +/- 18 months for full implementation.

- Map clients' needs and requirements
- Prepare technical requirement and documentation (kits, install guides, training guides, etc)
- Admin training (Web platform and available reporting tools)
- Parts and Inventory management

- Installers training
- Installations
- Users training (Web platform and reporting tools)
- Day 2 processes mapping and implementation
- Ongoing Quality assurance, audits, support

What was extremely important for the success of this project was a dedicated team from SkyHawk aligned with a dedicated team from the client.

SkyHawk Team - 1 Project Manager, 1 Project Coordinator, 1 level 2 support representative and 1 installations manager.
Client Team - 1 Project manager, 1 technical manager, 1 level 2 technical support representative.

A hands-on approach was important to initially map and plan the deployment/deliverables/requirement, followed by on-going technical and customer focused support to reduce issue resolution time.

Understanding of all technical installation requirements was fundamental to meet client expectations.

Open communication, physical presence and on-going planning meetings were/are very important to better manage the deployment and create a personal connection with the team.

Also, please see a copy of a Utility Case Study recently completed for another one of our utility clients.

a. Experience and qualifications of partners and subcontractors

Response

SkyHawk owns and has designed and built the cloud-based telematics software solution however a technical partner ecosystem is utilized for various aspects of our solution including the cloud-hosting, database managed services, mapping interface, in-vehicle data collection and communications hardware as well as interfaces to other third-party software applications as may be required by the client.

SkyHawk's partnerships, which support our main ConnectAnywhere cloud-based application, mainly consist of large, leading enterprise-based organizations such as Google, MongoDB and Amazon (AWS). The other major component of our technical partner ecosystem includes the companies that provide physical hardware included telematics modems, cabling and sensors which collect and transmit data from the vehicles. To ensure we are not exposed to any major supply chain issues (including those caused by COVID-19) SkyHawk holds a significant inventory of most all its major components for rapid and easy distribution to our clients.

Over the past 10 years SkyHawk has a holistic approach and developed a strong working relationship with selected partners and subcontractors to bridge the gap in offering our clients a comprehensive, one stop solution.

b. Description of Additional Integration and Consulting Services provided

Response

Vendor solution engineering/customization: While having specialized and feature matched system functionality is very important it is also important to have a telematics vendor that has the resources and capabilities to perform solution engineering. Our clients ultimately have requests and requirements which need custom development and attention to properly integrate with existing technologies and systems, including data exchange with other software applications. This cannot be achieved with "out-of-the-box" functionality. SkyHawk has a team of solution specialists and software engineers that can perform such tasks. Our clients have direct access to the Company who owns, designs, and develops the solution and not a solution reseller.

Rest API: ConnectAnywhere uses a REST API to easily integrate into third-part applications. The REST API provides simple read-only access to the most important data items in the ConnectAnywhere database, assets (both static attributes and current dynamic state) and messages (data points or transactions). It is an HTTP-based interface

implemented using REST (Representational State Transfer) principles, intended to be used by application developers who wish to transfer asset and message data to third-party systems or data management tools. By using JSON and HTTP/HTTPS the API can easily be accessed by an application using any of a variety of languages. The API is not event/notification based.

SkyHawk Telematics - SERVICE LEVEL AGREEMENT (SLA)

This “**Service Level Agreement**” is made pursuant to the AGREEMENT between Client (Buyer) and SkyHawk Telematics (as defined therein, the “**Agreement**”), to which this Service Level Agreement is attached as a Schedule. The terms of the Agreement are incorporated herein by reference. All capitalized terms not defined herein, shall have the meanings set forth in the Agreement. Actual Services must be separately acquired and paid for this Service Level Agreement to apply to any use of the Services.

1. Description of Services

1.1. Definitions – The following terms are defined for the purposes of this Service Level Agreement only:

- (a) “Critical” means any performance, operational or quality issues with BOSS Services, which result in the inability to use any of the BOSS Services for an extended period.
- (b) “Error” means any Failures or other performance, compatibility, operational, or quality issues, which result in the BOSS Software or Services not operating in accordance with the Agreement or the applicable Documentation and/or Specifications. An Error may have no appreciable impact on the operation or use of the BOSS Software or Services, or an Error may cause a “Minor Failure”, “Serious Failure”, or “Critical Failure”.
- (c) “Error Correction” means creating a permanent modification to the BOSS Software that enables the permanent resolution of an Error, implemented with an Update, Upgrade or Version. Error Corrections are implemented according to a BOSS testing, BOSS acceptance and BOSS implementation schedule.
- (d) “Help Desk” means BOSS’s telephone support line.
- (e) “Help Desk Services” means the telephone and service level management services provided by the Help Desk as described herein but excludes Training Services.
- (f) “Minor” means any performance, compatibility, operational, or quality issues that are not Critical Failures or Serious Failures. Minor failures can be an Error that does not interrupt critical workflow, are cosmetic in nature, or any Error for which a workaround is available.
- (g) “Patch” means the temporary repair or replacement of object or executable code versions of the BOSS Software on its production server(s) that enables the temporary resolution of an Error.
- (h) “Serious” means any performance, compatibility, operational, or quality issues with the BOSS Software that cause disruption to normal workflow and for which BOSS cannot provide a workaround. Serious Failures can be intermittent server downtime, user accessibility issues, or inability to access a key system function.
- (i) “Software Support and Maintenance Services” means the BOSS Services provided pursuant to Section 3 of this SLA.
- (j) “Update” means any new minor enhancement made to the BOSS Software issued by BOSS, which may also contain an Error Correction, and includes any update, patch installation, modification, renovation, refresh, enhancement, addition or substitution to the BOSS Software. Updates will be identified with a new update series number; for example 2.1.1 to 2.1.2.
- (k) “Upgrade” means any new major enhancement or grouping of enhancements, new functionality or revised or new modules made to the BOSS Software, issued by BOSS, and includes a collection of one or more Updates released as an Upgrade. Upgrades will be identified with a new Update series number; for example 2.1.2 to 2.2.0.
- (l) “Version” means any release of an Upgrade or collection of Upgrades to BOSS Software in respect of which BOSS uses a new version series number; for example 2.2.0 to 3.0.0
- (m) “Workaround” means a change in the procedures followed by Customer to avoid an Error without substantially impairing Customer’s access to or use of the BOSS Software.

2. Help Desk Services

2.1. The Help Desk Services set forth in this Section 2 of the SLA (the “**Help Desk Services**”) are provided in the categories indicated, based upon the selection of such BOSS Services in a Purchase Order, and payment of the applicable Service Fees in accordance with the Agreement.

2.2. BOSS shall staff a telephone Help Desk to provide assistance regarding the function, operation, and use of the BOSS Software, the Services and the Products, including:

- a) Reporting of issues;
- b) Assistance with diagnosing and resolving issues,
- c) Provision of Workarounds,
- d) Assistance other technical questions concerning the operation, maintenance, and use of the BOSS Software (but not training).
- e) In the event the Help Desk cannot resolve the issue, reference of the call to BOSS through the opening of a support ticket.

- 2.3. The Help Desk is available Monday to Friday 8:30am to 5pm EST or via email support@skyhawk.co . After Hours - call toll-free number below for the critical issues. Those calls will be dispatched to support personnel. Issues emailed to support after hours will be responded to next business day.

(a) North America: Toll-free number 1-844-4-24-7-SKYHAWK (1-844-424-7759) extension #2

3. **Service Response**

- 3.1. BOSS tracks customer reported issues and requests with support tickets. Each issue is assigned a support ticket with a unique identifier.
- 3.2. BOSS business days are 8:30 am to 5:00 pm EST, Monday to Friday, excluding Ontario statutory holidays.
- 3.3. For each support ticket for which BOSS identifies an Error as the cause, BOSS shall provide a Workaround or Patch and Error Correction in accordance with the guidelines in the chart below:

Error Severity	Acknowledgement	Response Time	Resolution
Minor	Upon Distributor or End Customer call to Help Desk or receipt of reply email from BOSS	BOSS shall respond within 1 business day	At the discretion of BOSS, will provide a Workaround and/or Error Correction in the next Version, Upgrade, or Update.
Serious	Upon Distributor or End Customer call to Help Desk or receipt of reply email from BOSS	BOSS shall respond the same business day, or if outside BOSS business hours, the next business day.	BOSS shall provide a Patch within 5 business days following response if possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.
Critical	Upon Distributor or End Customer call to Help Desk or receipt of reply email from BOSS	BOSS shall respond the same business day, or if outside BOSS business hours, will attempt to respond ASAP, but in all cases within 1 hour the next business day.	BOSS shall provide a Patch as soon as possible and shall provide a permanent Error Correction in the next Version, Upgrade or Update whichever comes first.

- 3.4. Distributor, on behalf of each End Customer or End Customer agrees to provide BOSS with all reasonably available information and materials requested by BOSS for use in replicating, diagnosing and correcting an Error reported by End Customer. End Customer must be using an Internet browser supported by the BOSS Software and must have continuously paid for Support and Maintenance Services acquiring the Service.
- 3.5. BOSS shall use commercially reasonable efforts to release Updates in a timely manner so as to keep the BOSS Software current with changes in operating systems, widely adopted Internet browsers, and other key computing platform elements on which, or in connection with which, the BOSS Software is used.

4. **Exclusions**

- 4.1. The BOSS Services provided hereunder shall not include:

- (a) Training Services;
- (b) Migration of data to or from other fleet and asset tracking systems; or
- (c) Custom Development Services,

which additional services may be provided pursuant to separate Quotation.

- 4.2. BOSS shall not be obliged to perform, and may suspend performance of, the BOSS Services, in the following instances:

- (a) Distributor or the End Customer has modified the installation environment of the BOSS Software, Products or Services without consent;
- (b) Distributor or the End Customer is in material breach of the Agreement, including failure to pay;
- (c) Distributor's or the End Customer's installation environment fails to meet the minimum requirements for the BOSS Software as set forth in the application Specifications; or

- (d) Distributor and the End Customer refuse to provide the necessary information to duplicate and/or assess the severity of the Error.

5. Service Level for SaaS Products (99.9% SLA)

This Service Level Agreement (the “SLA”) governs the use of all network infrastructure products and services (collectively, the “Services”) offered by SkyHawk Telematics, its parent company, and their affiliates and subsidiaries to its customers (“Customer”).

- 5.1. Service Commitment. SkyHawk Telematics is committed to providing services to its Customers at a standard of excellence commensurate with the best practice in the industry. Network uptime and server availability are of the highest importance. The following service levels are designed to assure Customers of ultimate performance and maximal uptime.
- 5.2. Server Hardware Replacement. SkyHawk Telematics guarantees the functioning of all hardware, including servers, CPU’s, cabling and associated server hardware, firewalls, load balancers, and storage area networks, and will replace any failed component at no cost to Customer within two hours following SkyHawk Telematics’ notification of the failure and SkyHawk Telematics’ identification of the failed hardware (the “Replacement Guarantee”). “Hardware” means the Processor(s), RAM, hard disk(s), motherboard, NIC card and other related hardware listed in the Service. The Replacement Guarantee does not include the time required to rebuild a RAID array or the reload of the operating systems and applications or changes to hardware during Maintenance, as defined below.
- 5.3. Power and HVAC Availability. SkyHawk Telematics guarantees that its power and HVAC systems will be available 100% of the time in a given month, excluding Maintenance, as defined below. “Infrastructure Downtime” means: (a) the SkyHawk Telematics power or HVAC systems are not available and (b) Customer submits a SkyHawk Telematics trouble ticket detailing the unavailability of the SkyHawk Telematics power or HVAC systems resulting in Customer downtime. Infrastructure Downtime does not include downtime issues related to power supplies on Customer’s servers, load balancers, or switches.
- 5.4. 99.9% Network Uptime. SkyHawk Telematics guarantees that the SkyHawk Telematics network will be available 99.9% of the time, excluding Maintenance, as defined below. Customer is eligible for a credit for Network Downtime for any breach of this guarantee, which can be verified by SkyHawk Telematics technical support team. “Network Downtime” is defined as an inability to transmit and receive data caused by failure of network equipment supplied by SkyHawk Telematics, excluding Maintenance, but including managed switches, routers, and cabling, and specifically excludes failure of network equipment and infrastructure owned or operated by the Public Switched Telephone Networks, cellular providers and/or satellite providers.
- 5.5. Maintenance. “Maintenance” means Scheduled Maintenance or Emergency Maintenance. “Scheduled Maintenance” means any maintenance in the SkyHawk Telematics datacenter of which Customer is notified at least 5 days in advance. “Emergency Maintenance” means any maintenance in the SkyHawk Telematics datacenter that: (a) in SkyHawk Telematics’ sole discretion, is necessary to avoid an immediate threat to the SkyHawk Telematics datacenter or Customer’s server and (b) of which Customer is notified.
- 5.6. Remedies. In the event SkyHawk Telematics fails to meet the Replacement Guarantee or customer experiences Infrastructure Downtime or Network Downtime as outlined herein, provided Customer follows the procedures outlined herein, SkyHawk Telematics will apply a credit (“Credit”) to Customer’s account in an amount equal to five percent (5%) of the Net MRC for the affected account for each hour of downtime or fraction thereof. “Net MRC” means the monthly recurring charge for the service, excluding cellular or satellite telecommunication fees, for the units impacted by the server(s) experiencing the issue(s). The Credits described in this SLA will be Customer’s exclusive remedy and SkyHawk Telematics’ entire liability for any breach of any warranty of performance or service contained in this SLA. In order to claim Credits, Customer must open a SkyHawk Telematics trouble ticket. All downtimes will be measured from the time the ticket is received and validated by SkyHawk Telematics to the time SkyHawk Telematics, in its sole discretion is able to resolve the issue. Customer may not receive more than one Credit per affected configuration per incident and in no event will Customer receive greater than one month’s Net MRC in Credit for any given month regardless of the number of incidents. Customer must be a SkyHawk Telematics customer in good standing to receive the Credit. No Credit will be applied to accounts that are past-due or for accounts that are canceled before the conditions for payment of the Credit are met. Upon cancellation of the Customer’s account, any outstanding or previously accrued Credits will be forfeited. Credits will be applied against purchases or renewals for which payment is due after the date the credit is applied. Credits will not be applied against past due balances.
- 5.7. Exceptions. Customer shall not be entitled to any Credit hereunder if Infrastructure Downtime or Network Downtime is caused by: (i) actions of the Customer or others authorized by Customer to use the Service under the Agreement; (ii) failure of applications or other software not provided by SkyHawk Telematics, (iii) the result of Maintenance activity, (iv) Denial of Service attack, hacker activity, or other malicious event or code targeted against SkyHawk Telematics or a SkyHawk Telematics Customer, or (vi) failure of any Network or Internet Infrastructure not owned or managed by SkyHawk Telematics. Server Hardware Replacement guarantee does not include time required to perform data restores and backups if applicable.

Attachment Q:
State of Utah Solicitation #CJ21-3
Client Reference Questionnaire

Preface:

- The information contained in this form will be applicable to Categories 3 of this RFP. It will be USCC's responsibility to identify which Category and Subcategories to which this Questionnaire pertains.
- The Information contained in this form will remain confidential and will be held to the State of Utah code and rules pertaining to confidentiality.

Vendor to fill out:

What Category and subcategory is this questionnaire for?

NASPO ValuePoint RFP for the Wireless Voice, Data & Accessories Category 3 (IoT) Refresh

Subcategory H: Snow & Ice Removal and Route Management

Subcategory O: Utility Operations, Monitoring and Support

Client Company name:	Skyhawk Clients, various, see below.
Client name of contact:	Response below
Client contact title:	Response below
Client is a daily user, occasional user, etc.:	Response below

Client to respond to Questions:

Dear USCC client:

USCC has identified your company as a reference able to provide feedback and information on their products and services. To assist the NASPO ValuePoint evaluation committee in evaluating the solution proposed by USCC, please complete this questionnaire in its entirety and return it to Chris Stokes no later than Friday, November 6th.

Thank you for your assistance in this process.

1. **For what services do you use USCC's product, and how long have you been USCC's customer?**

Responses below.

2. **Would you recommend USCC to other customers? Why?**

Responses below.

3. **Tell us about your initial installation and implementation experience. What did you think of USCC's ability to coordinate and manage the installation and implementation of your services? How responsive was USCC to requests or updates? Did USCC meet the required milestones/deadlines? If not, how delayed was USCC in completing tasks?**

Responses below.

- 4. Tell us about your customer service experience with USCC. Do they meet or exceed expectations/service level agreements? How did USCC deal with complaint resolution? Describe a situation in which USCC disappointed you and why. How did they respond?**

Responses below.

- 5. Does the product you purchased work the way you thought it would? How has it exceeded or fallen short of expectations?**

Responses below.

- 6. What do you wish had been different about your relationship with the USCC? If you could have changed one thing about the services or product, what would it have been?**

Responses below.

- 7. Is there anything else you think we should know about working with USCC or using USCC's products and services?**

Responses below.

- 8. Briefly describe other products and services that you have with this Vendor. What other relationships do you have with this Vendor if any?**

Responses below.

The following are a sampling of some governments clients that currently use the SkyHawk solution:

City of Portland, MA	North Dakota DOT
Town of Davenport, IO	Nova Scotia DOT
Town Urbandale, IO	County of Grande Prairie, AB
Rochester Hills, MI	City of Red Deer, AB
Midland County, MI	Federated Co-op, SK
Muskegon CRC, MI	Manitoba Hydro, MB
Midland CRC, MI	City of Hamilton, ON
City of St Clair Shores, MI	Hydro One Networks, ON
City of Kalamazoo, MI	Town of Flat Rock, NL
Stark County, OH	Hydro One Networks Inc., ON
The city of Brunswick, OH	Municipality of Chatham-Kent, ON
City of Joliet, IL	Hydro-Quebec, PQ

City of Springfield, MO	Town of Quispamsis, NB
City of West Fargo, ND	Town of Rothesay, NB
City of Pittsburgh, PA	Town of Dieppe, NB
City of Mount Pearl, NL	Portugal Cove-St. Philips, NL

Our references below will attest to SkyHawk's ability to deliver a superior product on time and in scope.

Reference (1)

New Hampshire Department of Transportation

7 Hazen Drive Concord, New Hampshire 03302-0483

David Gray

Winter Maintenance Program Specialist

(603) 485-3806 ext. 324

dgray@dot.state.nh.us

October 2016

Ongoing Project

GPS/AVL Winter Operations Solution. 65 Winter Operation Vehicles, and 24 Pickup Trucks - 89 Units

\$272,072.66

Reference (2)

City of Pittsburgh

414 Grant St. Pittsburgh, PA 15219

Chris Belasco

Project Manager

(412) 400-4505

chris.belasco@pittsburghpa.gov

October 2018

Ongoing Project

Complete Telematics Solution, Route Optimization, and Route Navigation system. 138 winter vehicles with a mix of approx. 350 heavy and light-duty vehicles - 488 Units

\$1.5 Million

Reference (3)

City of Hamilton

71 Main Street West, Hamilton, ON L8P 4Y5

Angela Storey

905-546-2424 ext. 6483

Angela.Storey@Hamilton.ca

April 2016

Ongoing Project

EMS vehicles that required integration with Bluetooth, Garmin devices for in-cab communication with Central Ambulance Control Centre and Ministry of Health and Long-Term Care reporting system as well as PTO reporting for lights, sirens.

Roads & Maintenance vehicles - design and creation of a Public access website, a mobile app for contractor specific application, integration to spreader controllers, and PTO status for winter snow plows.

Simple track and trace for Parks and Recreation, Animal Services, Buildings, By-laws, Cemeteries, Forestry, Hamilton Water, Horticulture - 750 Units to date.

\$5 Million

Reference (4)

Hydro One Networks Inc.

6975 Kenderry Gate | Mississauga, Ontario L5T 2Y1

Frank Currie

Manager - Fleet Services

(905) 696-7190 x 3315

frank.currie@hydroone.com

October 2013

December 2016

SkyHawk Telematics provided Hydro One with a complete telematics solution that facilitated fleet monitoring for multiple lines of business including Construction Services, Forestry, Provincial Lines, Fleet and Station Services. Over 5000 vehicles were installed with a dual-mode cellular/satellite solution to equip its fleet comprised of the boom truck, off-road and light-duty vehicles. The hardware installation and testing was a joint effort between the Hydro One mechanics and SkyHawk technicians, taking approximately 22 months to complete.

\$20 Million

Reference (5)

City of Davenport Iowa

226 West 4th Street, Davenport, IA52801

Art Bartleson

Director of Public Works Street Maintenance Supervisor

(563) 327-5114

abartleson@ci.davenport.ia.us

December 2015

November 2016

Installed SkyHawk 4G GPS/AVL system in late 2015 to replace an existing 2G system from another vendor. Davenport monitors their salt spreaders equipped with FA5100 and FA6100 controllers, graders, and supervisor vehicles. They use the live "Route Service" mapping overlay to monitor winter operations. SkyHawk has developed a printable route completion report for drivers coming on shift; testing at Davenport and other customers is helping developers maintain a timeline for an early fall release. City snow operations staff use SkyHawk to manage material usage, report costs and improve efficiency. Waste Department on boarded 2020 with 31 garbage trucks.

\$82,000.00



MA3696
Wireless Data, Voice, and Accessories
Attachment V
Category 3 Subcategory Definitions

Item	Application	Definition
A	Fleet Management	Allows the management of tasks associated with managing a fleet of vehicles through the use of telematics or remote sensing devices.
B	Mobile Device Management /Enterprise Mobility Management (MDM/EMM)	Mobile device management/enterprise mobility management (MDM/EMM) are solutions IT organizations use to manage and support end users' mobile devices, applications and data, and to enforce enterprise security policies.
E	Field Service Management	Systems that support the management of field service operations typically managing service orders, dispatching technicians, work planning, route optimization, time recording, maintenance data collection/analysis and other related functions.
F	Mobile Data Collection/Mobile Forms	A solution(s) that allow mobile users with cellular-equipped tablets or smartphones to collect data and possibly other information (e.g. pictures, videos, audio notes, locations, etc.), which is then sent over the cellular network to a cloud storage facility from which it can be accessed or downloaded by the customer.
G	Traffic Management and Intelligent Transport Systems (ITS)	Systems implemented by local governments to manage the flow of vehicle and potentially pedestrian traffic to reduce congestion, improve efficiency, reduce energy waste, improve safety and optimize road utilization.
H	Snow & Ice Removal and Route Management	Systems that would be used by government (and potentially other) agencies to manage road clearing operations resulting from snow storms or other weather events. Functions might include vehicle location, monitoring road conditions, dispatch, materials management, time clock, workforce monitoring, reporting, and other related functions.

I	Public Safety Systems	Any system that would be used by public safety organizations (e.g. Police, Fire, EMS, etc.) in executing their duties. Those functions might include multimodal communications, locating resources, managing responses, routing and dispatching, building and site intelligence, ongoing monitoring and detection systems, and other related functions.
J	IoT Management	Solutions to monitor, manage and maintain networks of Internet of Things (IoT) devices. Functions might include maintaining inventory, monitoring health/performance, measuring utilization, security maintenance, diagnostics and troubleshooting, downloading software/firmware updates, executing remote commands (e.g. turn off/on, reboot, etc.), logging/reporting, and other related functions.
M	Enterprise Messaging	A messaging solution offered as an alternative to traditional SMS/MMS and offering enterprise-grade security, archiving, and retrieval geared for the messaging requirements of organizations with stringent security requirements.
N	Secure LAN Access	A cellular wireless service providing a secure end-to-end virtual private network (VPN) type connection between a mobile device and to the customer's local area network (LAN).
O	Utility Operations, Monitoring and Support	Systems that support and monitor the operation of utilities including, but not limited to electrical generation and distribution, water, sewage and other utility services. Examples include, but are not limited to monitoring usage and consumption, improve energy and resource conservation, meter reading and distribution monitoring, automated operations and energy economics and sustainability compliance.



MA3696

Attachment W

Wireless Data, Voice and Accessories

Contractor Award Sheet

Contractor Name: US Cellular

Instructions: Please indicate below which categories of award apply to your proposal. Offerors may propose by state if desired in lieu of a National Award for Categories 3 and 4 (Regional). If Regional award is desired please indicate so on this attachment. Organizing your proposal so that each category of award is addressed separately would be preferable.

Category (subcategory)	Yes	No	Regional Award?
Category 3: Turnkey Wireless Solutions (Check this if any subcategories below)			
Category 3: Subcategory A: Fleet Management			
Category 3: Subcategory B: Mobile Device Management /Enterprise Mobility Management (MDM/EMM)			
Category 3: Subcategory E: Field Service Management			
Category 3: Subcategory F: Mobile Data Collection/Mobile Forms			
Category 3: Subcategory G: Traffic Management and Intelligent Transport Systems (ITS)			
Category 3: Subcategory H: Snow & Ice Removal and Route Management			
Category 3: Subcategory I: Public Safety Systems			
Category 3: Subcategory J: IoT Management			
Category 3: Subcategory M: Enterprise Messaging			
Category 3: Subcategory N: Secure LAN Access			
Category 3: Subcategory O: Utility Operations, Monitoring and Support			