Sourcewell

Solicitation Number: RFP #020624

CONTRACT

This Contract is between Sourcewell, 202 12th Street Northeast, P.O. Box 219, Staples, MN 56479 (Sourcewell) and Kajeet, Inc., 7901 Jones Branch Drive, Suite 350, McLean, VA 22102 (Supplier).

Sourcewell is a State of Minnesota local government unit and service cooperative created under the laws of the State of Minnesota (Minnesota Statutes Section 123A.21) that offers cooperative procurement solutions to government entities. Participation is open to eligible federal, state/province, and municipal governmental entities, higher education, K-12 education, nonprofit, tribal government, and other public entities located in the United States and Canada. Sourcewell issued a public solicitation for Private Wireless Services with Related Solutions from which Supplier was awarded a contract.

Supplier desires to contract with Sourcewell to provide equipment, products, or services to Sourcewell and the entities that access Sourcewell's cooperative purchasing contracts (Participating Entities).

1. TERM OF CONTRACT

A. EFFECTIVE DATE. This Contract is effective upon the date of the final signature below.

B. EXPIRATION DATE AND EXTENSION. This Contract expires May 7, 2028, unless it is cancelled sooner pursuant to Article 22. This Contract allows up to three additional one-year extensions upon the request of Sourcewell and written agreement by Supplier. Sourcewell retains the right to consider additional extensions beyond seven years as required under exceptional circumstances.

C. SURVIVAL OF TERMS. Notwithstanding any expiration or termination of this Contract, all payment obligations incurred prior to expiration or termination will survive, as will the following: Articles 11 through 14 survive the expiration or cancellation of this Contract. All other rights will cease upon expiration or termination of this Contract.

2. EQUIPMENT, PRODUCTS, OR SERVICES

A. EQUIPMENT, PRODUCTS, OR SERVICES. Supplier will provide the Equipment, Products, or Services as stated in its Proposal submitted under the Solicitation Number listed above. Supplier's Equipment, Products, or Services Proposal (Proposal) is attached and incorporated into this Contract.

All Equipment and Products provided under this Contract must be new and the current model. Supplier may offer close-out or refurbished Equipment or Products if they are clearly indicated in Supplier's product and pricing list. Unless agreed to by the Participating Entities in advance, Equipment or Products must be delivered as operational to the Participating Entity's site.

This Contract offers an indefinite quantity of sales, and while substantial volume is anticipated, sales and sales volume are not guaranteed.

B. WARRANTY. Supplier warrants that all Equipment, Products, and Services furnished are free from liens and encumbrances, and are free from defects in design, materials, and workmanship. In addition, Supplier warrants the Equipment, Products, and Services are suitable for and will perform in accordance with the ordinary use for which they are intended. Supplier's dealers and distributors must agree to assist the Participating Entity in reaching a resolution in any dispute over warranty terms with the manufacturer. Any manufacturer's warranty that extends beyond the expiration of the Supplier's warranty will be passed on to the Participating Entity.

C. DEALERS, DISTRIBUTORS, AND/OR RESELLERS. Upon Contract execution and throughout the Contract term, Supplier must provide to Sourcewell a current means to validate or authenticate Supplier's authorized dealers, distributors, or resellers relative to the Equipment, Products, and Services offered under this Contract, which will be incorporated into this Contract by reference. It is the Supplier's responsibility to ensure Sourcewell receives the most current information.

3. PRICING

All Equipment, Products, or Services under this Contract will be priced at or below the price stated in Supplier's Proposal.

When providing pricing quotes to Participating Entities, all pricing quoted must reflect a Participating Entity's total cost of acquisition. This means that the quoted cost is for delivered Equipment, Products, and Services that are operational for their intended purpose, and includes all costs to the Participating Entity's requested delivery location.

Regardless of the payment method chosen by the Participating Entity, the total cost associated with any purchase option of the Equipment, Products, or Services must always be disclosed in the pricing quote to the applicable Participating Entity at the time of purchase.

A. SHIPPING AND SHIPPING COSTS. All delivered Equipment and Products must be properly packaged. Damaged Equipment and Products may be rejected. If the damage is not readily apparent at the time of delivery, Supplier must permit the Equipment and Products to be returned within a reasonable time at no cost to Sourcewell or its Participating Entities. Participating Entities reserve the right to inspect the Equipment and Products at a reasonable time after delivery where circumstances or conditions prevent effective inspection of the Equipment and Products at the time of delivery. In the event of the delivery of nonconforming Equipment and Products, the Participating Entity will notify the Supplier as soon as possible and the Supplier will replace nonconforming Equipment and Products with conforming Equipment and Products that are acceptable to the Participating Entity.

Supplier must arrange for and pay for the return shipment on Equipment and Products that arrive in a defective or inoperable condition.

Sourcewell may declare the Supplier in breach of this Contract if the Supplier intentionally delivers substandard or inferior Equipment or Products.

B. SALES TAX. Each Participating Entity is responsible for supplying the Supplier with valid tax-exemption certification(s). When ordering, a Participating Entity must indicate if it is a tax-exempt entity.

C. HOT LIST PRICING. At any time during this Contract, Supplier may offer a specific selection of Equipment, Products, or Services at discounts greater than those listed in the Contract. When Supplier determines it will offer Hot List Pricing, it must be submitted electronically to Sourcewell in a line-item format. Equipment, Products, or Services may be added or removed from the Hot List at any time through a Sourcewell Price and Product Change Form as defined in Article 4 below.

Hot List program and pricing may also be used to discount and liquidate close-out and discontinued Equipment and Products as long as those close-out and discontinued items are clearly identified as such. Current ordering process and administrative fees apply. Hot List Pricing must be published and made available to all Participating Entities.

4. PRODUCT AND PRICING CHANGE REQUESTS

Supplier may request Equipment, Product, or Service changes, additions, or deletions at any time. All requests must be made in writing by submitting a signed Sourcewell Price and Product Change Request Form to the assigned Sourcewell Supplier Development Administrator. This approved form is available from the assigned Sourcewell Supplier Development Administrator. At a minimum, the request must:

- Identify the applicable Sourcewell contract number;
- Clearly specify the requested change;
- Provide sufficient detail to justify the requested change;
- Individually list all Equipment, Products, or Services affected by the requested change, along with the requested change (e.g., addition, deletion, price change); and
- Include a complete restatement of pricing documentation in Microsoft Excel with the effective date of the modified pricing, or product addition or deletion. The new pricing restatement must include all Equipment, Products, and Services offered, even for those items where pricing remains unchanged.

A fully executed Sourcewell Price and Product Change Request Form will become an amendment to this Contract and will be incorporated by reference.

5. PARTICIPATION, CONTRACT ACCESS, AND PARTICIPATING ENTITY REQUIREMENTS

A. PARTICIPATION. Sourcewell's cooperative contracts are available and open to public and nonprofit entities across the United States and Canada; such as federal, state/province, municipal, K-12 and higher education, tribal government, and other public entities.

The benefits of this Contract should be available to all Participating Entities that can legally access the Equipment, Products, or Services under this Contract. A Participating Entity's authority to access this Contract is determined through its cooperative purchasing, interlocal, or joint powers laws. Any entity accessing benefits of this Contract will be considered a Service Member of Sourcewell during such time of access. Supplier understands that a Participating Entity's use of this Contract is at the Participating Entity's sole convenience and Participating Entities reserve the right to obtain like Equipment, Products, or Services from any other source.

Supplier is responsible for familiarizing its sales and service forces with Sourcewell contract use eligibility requirements and documentation and will encourage potential participating entities to join Sourcewell. Sourcewell reserves the right to add and remove Participating Entities to its roster during the term of this Contract.

B. PUBLIC FACILITIES. Supplier's employees may be required to perform work at government-owned facilities, including schools. Supplier's employees and agents must conduct themselves in a professional manner while on the premises, and in accordance with Participating Entity policies and procedures, and all applicable laws.

6. PARTICIPATING ENTITY USE AND PURCHASING

A. ORDERS AND PAYMENT. To access the contracted Equipment, Products, or Services under this Contract, a Participating Entity must clearly indicate to Supplier that it intends to access this Contract; however, order flow and procedure will be developed jointly between Sourcewell and

Supplier. Typically, a Participating Entity will issue an order directly to Supplier or its authorized subsidiary, distributor, dealer, or reseller. If a Participating Entity issues a purchase order, it may use its own forms, but the purchase order should clearly note the applicable Sourcewell contract number. All Participating Entity orders under this Contract must be issued prior to expiration or cancellation of this Contract; however, Supplier performance, Participating Entity payment obligations, and any applicable warranty periods or other Supplier or Participating Entity obligations may extend beyond the term of this Contract.

Supplier's acceptable forms of payment are included in its attached Proposal. Participating Entities will be solely responsible for payment and Sourcewell will have no liability for any unpaid invoice of any Participating Entity.

B. ADDITIONAL TERMS AND CONDITIONS/PARTICIPATING ADDENDUM. Additional terms and conditions to a purchase order, or other required transaction documentation, may be negotiated between a Participating Entity and Supplier, such as job or industry-specific requirements, legal requirements (e.g., affirmative action or immigration status requirements), or specific local policy requirements. Some Participating Entities may require the use of a Participating Addendum, the terms of which will be negotiated directly between the Participating Entity and the Supplier or its authorized dealers, distributors, or resellers, as applicable. Any negotiated additional terms and conditions must never be less favorable to the Participating Entity than what is contained in this Contract.

C. SPECIALIZED SERVICE REQUIREMENTS. In the event that the Participating Entity requires service or specialized performance requirements not addressed in this Contract (such as e-commerce specifications, specialized delivery requirements, or other specifications and requirements), the Participating Entity and the Supplier may enter into a separate, standalone agreement, apart from this Contract. Sourcewell, including its agents and employees, will not be made a party to a claim for breach of such agreement.

D. TERMINATION OF ORDERS. Participating Entities may terminate an order, in whole or in part, immediately upon notice to Supplier in the event of any of the following events:

1. The Participating Entity fails to receive funding or appropriation from its governing body at levels sufficient to pay for the equipment, products, or services to be purchased; or
2. Federal, state, or provincial laws or regulations prohibit the purchase or change the Participating Entity's requirements.

E. GOVERNING LAW AND VENUE. The governing law and venue for any action related to a Participating Entity's order will be determined by the Participating Entity making the purchase.

7. CUSTOMER SERVICE

A. PRIMARY ACCOUNT REPRESENTATIVE. Supplier will assign an Account Representative to Sourcewell for this Contract and must provide prompt notice to Sourcewell if that person is changed. The Account Representative will be responsible for:

- Maintenance and management of this Contract;
- Timely response to all Sourcewell and Participating Entity inquiries; and
- Business reviews to Sourcewell and Participating Entities, if applicable.

B. BUSINESS REVIEWS. Supplier must perform a minimum of one business review with Sourcewell per contract year. The business review will cover sales to Participating Entities, pricing and contract terms, administrative fees, sales data reports, performance issues, supply issues, customer issues, and any other necessary information.

8. REPORT ON CONTRACT SALES ACTIVITY AND ADMINISTRATIVE FEE PAYMENT

A. CONTRACT SALES ACTIVITY REPORT. Each calendar quarter, Supplier must provide a contract sales activity report (Report) to the Sourcewell Supplier Development Administrator assigned to this Contract. Reports are due no later than 45 days after the end of each calendar quarter. A Report must be provided regardless of the number or amount of sales during that quarter (i.e., if there are no sales, Supplier must submit a report indicating no sales were made).

The Report must contain the following fields:

- Participating Entity Name (e.g., City of Staples Highway Department);
- Participating Entity Physical Street Address;
- Participating Entity City;
- Participating Entity State/Province;
- Participating Entity Zip/Postal Code;
- Participating Entity Contact Name;
- Participating Entity Contact Email Address;
- Participating Entity Contact Telephone Number;
- Sourcewell Assigned Entity/Participating Entity Number;
- Item Purchased Description;
- Item Purchased Price;
- Sourcewell Administrative Fee Applied; and
- Date Purchase was invoiced/sale was recognized as revenue by Supplier.

B. ADMINISTRATIVE FEE. In consideration for the support and services provided by Sourcewell, the Supplier will pay an administrative fee to Sourcewell on all Equipment, Products, and

Services provided to Participating Entities. The Administrative Fee must be included in, and not added to, the pricing. Supplier may not charge Participating Entities more than the contracted price to offset the Administrative Fee.

The Supplier will submit payment to Sourcewell for the percentage of administrative fee stated in the Proposal multiplied by the total sales of all Equipment, Products, and Services purchased by Participating Entities under this Contract during each calendar quarter. Payments should note the Supplier's name and Sourcewell-assigned contract number in the memo; and must be mailed to the address above "Attn: Accounts Receivable" or remitted electronically to Sourcewell's banking institution per Sourcewell's Finance department instructions. Payments must be received no later than 45 calendar days after the end of each calendar quarter.

Supplier agrees to cooperate with Sourcewell in auditing transactions under this Contract to ensure that the administrative fee is paid on all items purchased under this Contract.

In the event the Supplier is delinquent in any undisputed administrative fees, Sourcewell reserves the right to cancel this Contract and reject any proposal submitted by the Supplier in any subsequent solicitation. In the event this Contract is cancelled by either party prior to the Contract's expiration date, the administrative fee payment will be due no more than 30 days from the cancellation date.

9. AUTHORIZED REPRESENTATIVE

Sourcewell's Authorized Representative is its Chief Procurement Officer.

Supplier's Authorized Representative is the person named in the Supplier's Proposal. If Supplier's Authorized Representative changes at any time during this Contract, Supplier must promptly notify Sourcewell in writing.

10. AUDIT, ASSIGNMENT, AMENDMENTS, WAIVER, AND CONTRACT COMPLETE

A. AUDIT. Pursuant to Minnesota Statutes Section 16C.05, subdivision 5, the books, records, documents, and accounting procedures and practices relevant to this Contract are subject to examination by Sourcewell or the Minnesota State Auditor for a minimum of six years from the end of this Contract. This clause extends to Participating Entities as it relates to business conducted by that Participating Entity under this Contract.

B. ASSIGNMENT. Neither party may assign or otherwise transfer its rights or obligations under this Contract without the prior written consent of the other party and a fully executed assignment agreement. Such consent will not be unreasonably withheld. Any prohibited assignment will be invalid.

C. AMENDMENTS. Any amendment to this Contract must be in writing and will not be effective until it has been duly executed by the parties.

D. WAIVER. Failure by either party to take action or assert any right under this Contract will not be deemed a waiver of such right in the event of the continuation or repetition of the circumstances giving rise to such right. Any such waiver must be in writing and signed by the parties.

E. CONTRACT COMPLETE. This Contract represents the complete agreement between the parties. No other understanding regarding this Contract, whether written or oral, may be used to bind either party. For any conflict between the attached Proposal and the terms set out in Articles 1-22 of this Contract, the terms of Articles 1-22 will govern.

F. RELATIONSHIP OF THE PARTIES. The relationship of the parties is one of independent contractors, each free to exercise judgment and discretion with regard to the conduct of their respective businesses. This Contract does not create a partnership, joint venture, or any other relationship such as master-servant, or principal-agent.

11. INDEMNITY AND HOLD HARMLESS

Supplier must indemnify, defend, save, and hold Sourcewell and its Participating Entities, including their agents and employees, harmless from any claims or causes of action, including attorneys' fees incurred by Sourcewell or its Participating Entities, arising out of any act or omission in the performance of this Contract by the Supplier or its agents or employees; this indemnification includes injury or death to person(s) or property alleged to have been caused by some defect in the Equipment, Products, or Services under this Contract to the extent the Equipment, Product, or Service has been used according to its specifications. Sourcewell's responsibility will be governed by the State of Minnesota's Tort Liability Act (Minnesota Statutes Chapter 466) and other applicable law.

12. GOVERNMENT DATA PRACTICES

Supplier and Sourcewell must comply with the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, as it applies to all data provided by or provided to Sourcewell under this Contract and as it applies to all data created, collected, received, maintained, or disseminated by the Supplier under this Contract.

13. INTELLECTUAL PROPERTY, PUBLICITY, MARKETING, AND ENDORSEMENT

A. INTELLECTUAL PROPERTY

1. *Grant of License.* During the term of this Contract:

    a. Sourcewell grants to Supplier a royalty-free, worldwide, non-exclusive right and license to use the trademark(s) provided to Supplier by Sourcewell in advertising and

promotional materials for the purpose of marketing Sourcewell's relationship with Supplier.

b. Supplier grants to Sourcewell a royalty-free, worldwide, non-exclusive right and license to use Supplier's trademarks in advertising and promotional materials for the purpose of marketing Supplier's relationship with Sourcewell.

2. *Limited Right of Sublicense*. The right and license granted herein includes a limited right of each party to grant sublicenses to their respective subsidiaries, distributors, dealers, resellers, marketing representatives, and agents (collectively "Permitted Sublicensees") in advertising and promotional materials for the purpose of marketing the Parties' relationship to Participating Entities. Any sublicense granted will be subject to the terms and conditions of this Article. Each party will be responsible for any breach of this Article by any of their respective sublicensees.

3. *Use; Quality Control.*

a. Neither party may alter the other party's trademarks from the form provided and must comply with removal requests as to specific uses of its trademarks or logos.

b. Each party agrees to use, and to cause its Permitted Sublicensees to use, the other party's trademarks only in good faith and in a dignified manner consistent with such party's use of the trademarks. Upon written notice to the breaching party, the breaching party has 30 days of the date of the written notice to cure the breach or the license will be terminated.

4. *Termination*. Upon the termination of this Contract for any reason, each party, including Permitted Sublicensees, will have 30 days to remove all Trademarks from signage, websites, and the like bearing the other party's name or logo (excepting Sourcewell's pre-printed catalog of suppliers which may be used until the next printing). Supplier must return all marketing and promotional materials, including signage, provided by Sourcewell, or dispose of it according to Sourcewell's written directions.

B. PUBLICITY. Any publicity regarding the subject matter of this Contract must not be released without prior written approval from the Authorized Representatives. Publicity includes notices, informational pamphlets, press releases, research, reports, signs, and similar public notices prepared by or for the Supplier individually or jointly with others, or any subcontractors, with respect to the program, publications, or services provided resulting from this Contract.

C. MARKETING. Any direct advertising, marketing, or offers with Participating Entities must be approved by Sourcewell. Send all approval requests to the Sourcewell Supplier Development Administrator assigned to this Contract.

D. ENDORSEMENT. The Supplier must not claim that Sourcewell endorses its Equipment, Products, or Services.

14. GOVERNING LAW, JURISDICTION, AND VENUE

The substantive and procedural laws of the State of Minnesota will govern this Contract. Venue for all legal proceedings arising out of this Contract, or its breach, must be in the appropriate state court in Todd County, Minnesota or federal court in Fergus Falls, Minnesota.

15. FORCE MAJEURE

Neither party to this Contract will be held responsible for delay or default caused by acts of God or other conditions that are beyond that party's reasonable control. A party defaulting under this provision must provide the other party prompt written notice of the default.

16. SEVERABILITY

If any provision of this Contract is found by a court of competent jurisdiction to be illegal, unenforceable, or void then both parties will be relieved from all obligations arising from that provision. If the remainder of this Contract is capable of being performed, it will not be affected by such determination or finding and must be fully performed.

17. PERFORMANCE, DEFAULT, AND REMEDIES

A. PERFORMANCE. During the term of this Contract, the parties will monitor performance and address unresolved contract issues as follows:

1. *Notification.* The parties must promptly notify each other of any known dispute and work in good faith to resolve such dispute within a reasonable period of time. If necessary, Sourcewell and the Supplier will jointly develop a short briefing document that describes the issue(s), relevant impact, and positions of both parties.
2. *Escalation.* If parties are unable to resolve the issue in a timely manner, as specified above, either Sourcewell or Supplier may escalate the resolution of the issue to a higher level of management. The Supplier will have 30 calendar days to cure an outstanding issue.
3. *Performance while Dispute is Pending*. Notwithstanding the existence of a dispute, the Supplier must continue without delay to carry out all of its responsibilities under the Contract that are not affected by the dispute. If the Supplier fails to continue without delay to perform its responsibilities under the Contract, in the accomplishment of all undisputed work, the Supplier will bear any additional costs incurred by Sourcewell and/or its Participating Entities as a result of such failure to proceed.

B. DEFAULT AND REMEDIES. Either of the following constitutes cause to declare this Contract, or any Participating Entity order under this Contract, in default:

1. Nonperformance of contractual requirements, or
2. A material breach of any term or condition of this Contract.

The party claiming default must provide written notice of the default, with 30 calendar days to cure the default. Time allowed for cure will not diminish or eliminate any liability for liquidated or other damages. If the default remains after the opportunity for cure, the non-defaulting party may:

- Exercise any remedy provided by law or equity, or
- Terminate the Contract or any portion thereof, including any orders issued against the Contract.

18. INSURANCE

A. REQUIREMENTS. At its own expense, Supplier must maintain insurance policy(ies) in effect at all times during the performance of this Contract with insurance company(ies) licensed or authorized to do business in the State of Minnesota having an "AM BEST" rating of A- or better, with coverage and limits of insurance not less than the following:

1. *Workers' Compensation and Employer's Liability.*
Workers' Compensation: As required by any applicable law or regulation.
Employer's Liability Insurance: must be provided in amounts not less than listed below:
Minimum limits:
$500,000 each accident for bodily injury by accident
$500,000 policy limit for bodily injury by disease
$500,000 each employee for bodily injury by disease

2. *Commercial General Liability Insurance.* Supplier will maintain insurance covering its operations, with coverage on an occurrence basis, and must be subject to terms no less broad than the Insurance Services Office ("ISO") Commercial General Liability Form CG0001 (2001 or newer edition), or equivalent. At a minimum, coverage must include liability arising from premises, operations, bodily injury and property damage, independent contractors, products-completed operations including construction defect, contractual liability, blanket contractual liability, and personal injury and advertising injury. All required limits, terms and conditions of coverage must be maintained during the term of this Contract.
Minimum Limits:
$1,000,000 each occurrence Bodily Injury and Property Damage
$1,000,000 Personal and Advertising Injury
$2,000,000 aggregate for products liability-completed operations
$2,000,000 general aggregate

3. *Commercial Automobile Liability Insurance.* During the term of this Contract, Supplier will maintain insurance covering all owned, hired, and non-owned automobiles in limits of liability not less than indicated below. The coverage must be subject to terms

no less broad than ISO Business Auto Coverage Form CA 0001 (2010 edition or newer), or equivalent.

Minimum Limits:
$1,000,000 each accident, combined single limit

4. *Umbrella Insurance*. During the term of this Contract, Supplier will maintain umbrella coverage over Employer's Liability, Commercial General Liability, and Commercial Automobile.

Minimum Limits:
$2,000,000

5. *Professional/Technical, Errors and Omissions, and/or Miscellaneous Professional Liability*. During the term of this Contract, Supplier will maintain coverage for all claims the Supplier may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to Supplier's professional services required under this Contract.

Minimum Limits:
$2,000,000 per claim or event
$2,000,000 – annual aggregate

6. *Network Security and Privacy Liability Insurance*. During the term of this Contract, Supplier will maintain coverage for network security and privacy liability. The coverage may be endorsed on another form of liability coverage or written on a standalone policy. The insurance must cover claims which may arise from failure of Supplier's security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of not public data – including but not limited to, confidential or private information, transmission of a computer virus, or denial of service.

Minimum limits:
$2,000,000 per occurrence
$2,000,000 annual aggregate

Failure of Supplier to maintain the required insurance will constitute a material breach entitling Sourcewell to immediately terminate this Contract for default.

B. CERTIFICATES OF INSURANCE. Prior to commencing under this Contract, Supplier must furnish to Sourcewell a certificate of insurance, as evidence of the insurance required under this Contract. Prior to expiration of the policy(ies), renewal certificates must be mailed to Sourcewell, 202 12th Street Northeast, P.O. Box 219, Staples, MN 56479 or sent to the Sourcewell Supplier Development Administrator assigned to this Contract. The certificates must be signed by a person authorized by the insurer(s) to bind coverage on their behalf.

Failure to request certificates of insurance by Sourcewell, or failure of Supplier to provide certificates of insurance, in no way limits or relieves Supplier of its duties and responsibilities in this Contract.

C. ADDITIONAL INSURED ENDORSEMENT AND PRIMARY AND NON-CONTRIBUTORY INSURANCE CLAUSE. Supplier agrees to list Sourcewell and its Participating Entities, including their officers, agents, and employees, as an additional insured under the Supplier's commercial general liability insurance policy with respect to liability arising out of activities, "operations," or "work" performed by or on behalf of Supplier, and products and completed operations of Supplier. The policy provision(s) or endorsement(s) must further provide that coverage is primary and not excess over or contributory with any other valid, applicable, and collectible insurance or self-insurance in force for the additional insureds.

D. WAIVER OF SUBROGATION. Supplier waives and must require (by endorsement or otherwise) all its insurers to waive subrogation rights against Sourcewell and other additional insureds for losses paid under the insurance policies required by this Contract or other insurance applicable to the Supplier or its subcontractors. The waiver must apply to all deductibles and/or self-insured retentions applicable to the required or any other insurance maintained by the Supplier or its subcontractors. Where permitted by law, Supplier must require similar written express waivers of subrogation and insurance clauses from each of its subcontractors.

E. UMBRELLA/EXCESS LIABILITY/SELF-INSURED RETENTION. The limits required by this Contract can be met by either providing a primary policy or in combination with umbrella/excess liability policy(ies), or self-insured retention.

19. COMPLIANCE

A. LAWS AND REGULATIONS. All Equipment, Products, or Services provided under this Contract must comply fully with applicable federal laws and regulations, and with the laws in the states and provinces in which the Equipment, Products, or Services are sold.

B. LICENSES. Supplier must maintain a valid and current status on all required federal, state/provincial, and local licenses, bonds, and permits required for the operation of the business that the Supplier conducts with Sourcewell and Participating Entities.

20. BANKRUPTCY, DEBARMENT, OR SUSPENSION CERTIFICATION

Supplier certifies and warrants that it is not in bankruptcy or that it has previously disclosed in writing certain information to Sourcewell related to bankruptcy actions. If at any time during this Contract Supplier declares bankruptcy, Supplier must immediately notify Sourcewell in writing.

Supplier certifies and warrants that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from programs operated by the State of Minnesota; the United States federal government or the Canadian government, as applicable; or any Participating Entity. Supplier certifies and warrants that neither it nor its principals have been convicted of a criminal offense related to the subject matter of this Contract. Supplier further warrants that it will provide immediate written notice to Sourcewell if this certification changes at any time.

21. PROVISIONS FOR NON-UNITED STATES FEDERAL ENTITY PROCUREMENTS UNDER UNITED STATES FEDERAL AWARDS OR OTHER AWARDS

Participating Entities that use United States federal grant or FEMA funds to purchase goods or services from this Contract may be subject to additional requirements including the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 C.F.R. § 200. Participating Entities may have additional requirements based on specific funding source terms or conditions. Within this Article, all references to "federal" should be interpreted to mean the United States federal government. The following list only applies when a Participating Entity accesses Supplier's Equipment, Products, or Services with United States federal funds.

A. EQUAL EMPLOYMENT OPPORTUNITY. Except as otherwise provided under 41 C.F.R. § 60, all contracts that meet the definition of "federally assisted construction contract" in 41 C.F.R. § 60-1.3 must include the equal opportunity clause provided under 41 C.F.R. §60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 C.F.R. §, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 C.F.R. § 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." The equal opportunity clause is incorporated herein by reference.

B. DAVIS-BACON ACT, AS AMENDED (40 U.S.C. § 3141-3148). When required by federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. § 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 C.F.R. § 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non-federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-federal entity must report all suspected or reported violations to the federal awarding agency. The contracts must also include a provision for compliance with

the Copeland "Anti-Kickback" Act (40 U.S.C. § 3145), as supplemented by Department of Labor regulations (29 C.F.R. § 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-federal entity must report all suspected or reported violations to the federal awarding agency. Supplier must be in compliance with all applicable Davis-Bacon Act provisions.

C. CONTRACT WORK HOURS AND SAFETY STANDARDS ACT (40 U.S.C. § 3701-3708). Where applicable, all contracts awarded by the non-federal entity in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. §§ 3702 and 3704, as supplemented by Department of Labor regulations (29 C.F.R. § 5). Under 40 U.S.C. § 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. § 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence. This provision is hereby incorporated by reference into this Contract. Supplier certifies that during the term of an award for all contracts by Sourcewell resulting from this procurement process, Supplier must comply with applicable requirements as referenced above.

D. RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT. If the federal award meets the definition of "funding agreement" under 37 C.F.R. § 401.2(a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 C.F.R. § 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency. Supplier certifies that during the term of an award for all contracts by Sourcewell resulting from this procurement process, Supplier must comply with applicable requirements as referenced above.

E. CLEAN AIR ACT (42 U.S.C. § 7401-7671Q.) AND THE FEDERAL WATER POLLUTION CONTROL ACT (33 U.S.C. § 1251-1387). Contracts and subgrants of amounts in excess of $150,000 require the non-federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. § 7401- 7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. § 1251- 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

Supplier certifies that during the term of this Contract will comply with applicable requirements as referenced above.

F. DEBARMENT AND SUSPENSION (EXECUTIVE ORDERS 12549 AND 12689). A contract award (see 2 C.F.R. § 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 C.F.R. §180 that implement Executive Orders 12549 (3 C.F.R. § 1986 Comp., p. 189) and 12689 (3 C.F.R. § 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. Supplier certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency.

G. BYRD ANTI-LOBBYING AMENDMENT, AS AMENDED (31 U.S.C. § 1352). Suppliers must file any required certifications. Suppliers must not have used federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Suppliers must disclose any lobbying with non-federal funds that takes place in connection with obtaining any federal award. Such disclosures are forwarded from tier to tier up to the non-federal award. Suppliers must file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 U.S.C. § 1352).

H. RECORD RETENTION REQUIREMENTS. To the extent applicable, Supplier must comply with the record retention requirements detailed in 2 C.F.R. § 200.333. The Supplier further certifies that it will retain all records as required by 2 C.F.R. § 200.333 for a period of 3 years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

I. ENERGY POLICY AND CONSERVATION ACT COMPLIANCE. To the extent applicable, Supplier must comply with the mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act.

J. BUY AMERICAN PROVISIONS COMPLIANCE. To the extent applicable, Supplier must comply with all applicable provisions of the Buy American Act. Purchases made in accordance with the Buy American Act must follow the applicable procurement rules calling for free and open competition.

K. ACCESS TO RECORDS (2 C.F.R. § 200.336). Supplier agrees that duly authorized representatives of a federal agency must have access to any books, documents, papers and

records of Supplier that are directly pertinent to Supplier's discharge of its obligations under this Contract for the purpose of making audits, examinations, excerpts, and transcriptions. The right also includes timely and reasonable access to Supplier's personnel for the purpose of interview and discussion relating to such documents.

L. PROCUREMENT OF RECOVERED MATERIALS (2 C.F.R. § 200.322). A non-federal entity that is a state agency or agency of a political subdivision of a state and its contractors must comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 C.F.R. § 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

M. FEDERAL SEAL(S), LOGOS, AND FLAGS. The Supplier cannot use the seal(s), logos, crests, or reproductions of flags or likenesses of Federal agency officials without specific pre-approval.

N. NO OBLIGATION BY FEDERAL GOVERNMENT. The U.S. federal government is not a party to this Contract or any purchase by a Participating Entity and is not subject to any obligations or liabilities to the Participating Entity, Supplier, or any other party pertaining to any matter resulting from the Contract or any purchase by an authorized user.

O. PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS OR RELATED ACTS. The Contractor acknowledges that 31 U.S.C. 38 (Administrative Remedies for False Claims and Statements) applies to the Supplier's actions pertaining to this Contract or any purchase by a Participating Entity.

P. FEDERAL DEBT. The Supplier certifies that it is non-delinquent in its repayment of any federal debt. Examples of relevant debt include delinquent payroll and other taxes, audit disallowance, and benefit overpayments.

Q. CONFLICTS OF INTEREST. The Supplier must notify the U.S. Office of General Services, Sourcewell, and Participating Entity as soon as possible if this Contract or any aspect related to the anticipated work under this Contract raises an actual or potential conflict of interest (as described in 2 C.F.R. Part 200). The Supplier must explain the actual or potential conflict in writing in sufficient detail so that the U.S. Office of General Services, Sourcewell, and Participating Entity are able to assess the actual or potential conflict; and provide any additional information as necessary or requested.

R. U.S. EXECUTIVE ORDER 13224. The Supplier, and its subcontractors, must comply with U.S. Executive Order 13224 and U.S. Laws that prohibit transactions with and provision of resources and support to individuals and organizations associated with terrorism.

S. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT. To the extent applicable, Supplier certifies that during the term of this Contract it will comply with applicable requirements of 2 C.F.R. § 200.216.

T. DOMESTIC PREFERENCES FOR PROCUREMENTS. To the extent applicable, Supplier certifies that during the term of this Contract will comply with applicable requirements of 2 C.F.R. § 200.322.

22. CANCELLATION

Sourcewell or Supplier may cancel this Contract at any time, with or without cause, upon 60 days' written notice to the other party. However, Sourcewell may cancel this Contract immediately upon discovery of a material defect in any certification made in Supplier's Proposal. Cancellation of this Contract does not relieve either party of financial, product, or service obligations incurred or accrued prior to cancellation.

Sourcewell

DocuSigned by:
By: Jeremy Schwartz
C0FD2A139D06489...
Jeremy Schwartz
Title: Chief Procurement Officer
Date: 5/6/2024 | 11:29 AM CDT

Kajeet, Inc.

DocuSigned by:
By: Guy Abramovitz
C9C41A2F6B36409...
Guy Abramovitz
Title: CFO
Date: 5/6/2024 | 8:40 AM PDT

RFP 020624 - Private Wireless Services with Related Solutions

Vendor Details

Company Name:	Kajeet, Inc.
Address:	7901 JONES BRANCH DRIVE STE 350 McLean, VA 22102
Contact:	Catherine Holz
Email:	publicsectorpmo@kajeet.com
Phone:	240-482-3500
HST#:	

Submission Details

Created On:	Friday January 12, 2024 08:58:32
Submitted On:	Tuesday February 20, 2024 15:32:42
Submitted By:	Jamaal Smith
Email:	jsmith@kajeet.com
Transaction #:	5aab7989-01d6-4bdc-bd16-8424b14791a7
Submitter's IP Address:	35.145.203.16

Specifications

Table 1: Proposer Identity & Authorized Representatives

General Instructions (applies to all Tables) Sourcewell prefers a brief but thorough response to each question. Do not merely attach additional documents to your response without also providing a substantive response. Do not leave answers blank; respond "N/A" if the question does not apply to you (preferably with an explanation).

Line Item	Question	Response *	
1	Proposer Legal Name (one legal entity only): (In the event of award, will execute the resulting contract as "Supplier")	Kajeet, Inc.	*
2	Identify all subsidiary entities of the Proposer whose equipment, products, or services are included in the Proposal.	N/A. Kajeet has no subsidiary entities.	*
3	Identify all applicable assumed names or DBA names of the Proposer or Proposer's subsidiaries in Line 1 or Line 2 above.	N/A Kajeet has no current DBA names.	*
4	Provide your CAGE code or Unique Entity Identifier (SAM):	7Q8F0	*
5	Proposer Physical Address:	7901 Jones Branch Drive, Suite 350 McLean, VA 22102	*
6	Proposer website address (or addresses):	www.kajeet.com	*
7	Proposer's Authorized Representative (name, title, address, email address & phone) (The representative must have authority to sign the "Proposer's Assurance of Compliance" on behalf of the Proposer and, in the event of award, will be expected to execute the resulting contract):	Guy Abramovitz, CFO 7901 Jones Branch Drive, Ste 350, McLean, VA 22102 gabramovitz@kajeet.com 215-694-0245	*
8	Proposer's primary contact for this proposal (name, title, address, email address & phone):	Jamaal Smith, VP of Sales & Business Development 7901 Jones Branch Drive, Ste 350, McLean, VA 22102 jsmith@kajeet.com 845-668-1000	*
9	Proposer's other contacts for this proposal, if any (name, title, address, email address & phone):	Michael Carr, Senior Director 7901 Jones Branch Drive, Ste 350, McLean, VA 22102 mcarr@kajeet.com 703-930-8475	

Table 2: Company Information and Financial Strength

Line Item	Question	Response *	

10	Provide a brief history of your company, including your company's core values, business philosophy, and industry longevity related to the requested equipment, products or services.	At Kajeet, we believe that Internet access is a basic human right and in providing connectivity for good. For the 19 million people in the U.S. who still lack home broadband access, the world of online opportunities remains out of reach. We partner with our customers to create digitally inclusive communities – especially for those who are disproportionately affected by the digital divide. Kajeet is an award-winning company with 41 patents. In addition to IoT Evolution, DCA Live Red Hot Companies, and Community Builder Awards, in November of this year, Kajeet received the 2022 Best Practices New Product Innovation Award from Frost & Sullivan. This award is a result of Frost & Sullivan's analyst teams' efforts to independently identify businesses paving the way in significant new growth areas in technology. Kajeet® is a leading provider of wireless connectivity, software and hardware solutions that deliver secure, reliable, and managed wireless solutions to over 3,000 businesses, schools and districts, and state and local governments. Kajeet's Private 5G Platform simplifies private wireless to allow education and enterprise customers to easily build and manage their own private wireless networks. Kajeet is the only service provider in the industry to offer Sentinel®, a smart, simple, and secure single pane of glass for a wireless device, SIM, and network management. Sentinel includes AI/ML visibility into real-time data usage, policy control management, custom content filters for added security and hybrid private and public network access across all major North American wireless networks and on multiple licensed and unlicensed networks. Kajeet holds 41 U.S. patents in mobile technologies.	*
11	What are your company's expectations in the event of an award?	Kajeet's expectations are similar to our other existing procurement vehicle contracts whereby we intend to promote the Sourcewell agreement to grow/expand our business. We expect that an award from Sourcewell will present us with opportunities to identify new opportunities to expand our footprint and earn new customers.	*
12	Demonstrate your financial strength and stability with meaningful data. This could include such items as financial statements, SEC filings, credit and bond ratings, letters of credit, and detailed reference letters. Upload supporting documents (as applicable) in the document upload section of your response.	Kajeet is a privately held company that has been in business for 20 years. The company is headquartered in McLean, VA, and also has a warehouse in Phoenix, AZ. Kajeet is financially healthy, with continued historical growth, and revenue of approximately $105 million in 2022.	*

13	What is your US market share for the solutions that you are proposing?	In the competitive landscape of wireless solutions, Kajeet stands as the premier provider, uniquely offering a comprehensive trifecta of services in the United States. Our distinctive approach encompasses three key wireless solution offerings: Public Wireless & IoT Connectivity: Kajeet is the exclusive provider of Public Wireless & IoT Connectivity, partnering with major carriers such as AT&T, T-Mobile, Verizon, and U.S. Cellular. This extensive network coverage ensures a robust and reliable connectivity foundation for our clients. Private Wireless Connectivity: Our innovative solutions empower clients to establish, operate, and manage their own cellular networks. Kajeet leads the industry in facilitating Private Wireless Connectivity, offering a tailored and secure approach to meet diverse connectivity needs. Neutral Host Connectivity: Leveraging CBRS MOCN Neutral Host, Kajeet excels in enhancing in-building cellular connectivity. This cutting-edge technology plays a pivotal role in our commitment to providing Neutral Host Connectivity, especially in educational settings. Market Leadership Achievements: Kajeet holds a dominant position as the leader in multi-carrier student wireless connectivity, playing a pivotal role in narrowing the digital divide across the nation. Recognized for excellence, we are at the forefront of supplying WiFi access on school buses nationwide, showcasing our commitment to enhancing connectivity in educational environments. With over 40 successfully completed private wireless deployments, Kajeet is a trailblazer in the education sector, setting the standard for Private Wireless Networks. Industry Acknowledgments: Frost & Sullivan Global Private Wireless Networks For Education New Product Innovation Award 2023 Mobile Breakthrough Innovation Award 2023 IoT Evolution Award for Neutral Host Networking 2023 Broadband Summit Award for Excellence in Wireless Neutral Host Networking In summary, Kajeet proudly holds the leadership position in the U.S. market, offering unparalleled expertise in multi-carrier connectivity, private wireless solutions, and cutting-edge neutral host technology. Our proven track record and industry accolades underscore our commitment to excellence in wireless connectivity across diverse sectors.	*
14	What is your Canadian market share for the solutions that you are proposing?	None at this time.	*
15	Has your business ever petitioned for bankruptcy protection? If so, explain in detail.	No.	*
16	How is your organization best described: is it a manufacturer, a distributor/dealer/reseller, or a service provider? Answer whichever question (either a) or b) just below) best applies to your organization. a) If your company is best described as a distributor/dealer/reseller (or similar entity), provide your written authorization to act as a distributor/dealer/reseller for the manufacturer of the products proposed in this RFP. If applicable, is your dealer network independent or company owned? b) If your company is best described as a manufacturer or service provider, describe your relationship with your sales and service force and with your dealer network in delivering the products and services proposed in this RFP. Are these individuals your employees, or the employees of a third party?	Kajeet is best described as a distributor/dealer/reseller. We have certified partners that perform Installation and other services. Kajeet has on staff multiple OnGo Alliance Certified Professional Installers (CPI). This certification is required to deploy CBRS Radios in the United States. Kajeet's team of engineers are certified to install, configure and manage the following manufacturers: Samsung Baicells Airspan Cisco Cradlepoint	*

17	If applicable, provide a detailed explanation outlining the licenses and certifications that are both required to be held, and actually held, by your organization (including third parties and subcontractors that you use) in pursuit of the business contemplated by this RFP.	Kajeet has on staff multiple OnGo Alliance Certified Professional Installers (CPI). This certification is required to deploy CBRS Radios in the United States. Kajeet's team of engineers are certified to install, configure and manage the following manufacturers: Samsung Baicells Airspan Cisco Cradlepoint Kajeet holds the following security certification: SOC Type2 I & II.	*
18	Provide all "Suspension or Debarment" information that has applied to your organization during the past ten years.	N/A. Kajeet has not been suspended or debarred during the past ten years.	*

Table 3: Industry Recognition & Marketplace Success

Line Item	Question	Response *	
19	Describe any relevant industry awards or recognition that your company has received in the past five years	-2022 Frost & Sullivan New Product Innovation Award -2022 Leading Lights Award Finalist for Best Public-Private Partnership -2022 Mobile Breakthrough Award for Global Innovation Leadership -2023 IoT Evolution Private Wireless Network Innovation Award -2023 U.S. Broadband Award winner in the Wireless Neutral Host Networks category	*
20	What percentage of your sales are to the governmental sector in the past three years	None	*
21	What percentage of your sales are to the education sector in the past three years	70%	*
22	List any state, provincial, or cooperative purchasing contracts that you hold. What is the annual sales volume for each of these contracts over the past three years?	AEPA - $20M, Buyboard - $300K, DIR-TEXAN $50K, PEPPM - $5M, HCDE/Choice Partners	*
23	List any GSA contracts or Standing Offers and Supply Arrangements (SOSA) that you hold. What is the annual sales volume for each of these contracts over the past three years?	Not applicable	*

Table 4: References/Testimonials

Line Item 24. Supply reference information from three customers who are eligible to be Sourcewell participating entities and for whom you have performed projects relevant to private wireless services. .

Entity Name *	Contact Name *	Phone Number *	
Nebraska Indian Community College (NICC)	Justin Kocian - Chief Information Officer / Title III Project Director	402-241-5981	*
Colusa County Office of Education (CCOE)	Alexandar Evans - Director of Technology	530-458-0350 x10355	*
Keystone Metro Fiber (KMF)	Richard Kolsby - Chief Technical Officer	404-229-8953	*

Table 5: Top Five Government or Education Customers

Line Item 25. Provide a list of your top five government, education, or non-profit customers (entity name is optional), including entity type, the state or province the entity is located in, scope of the project(s), size of transaction(s), and dollar volumes from the past three years.

Entity Name	Entity Type *	State / Province *	Scope of Work *	Size of Transactions *	Dollar Volume Past Three Years *	
NICC	Education	Nebraska - NE	NICC provides a culturally infused learning environment dedicated to bringing state-of-the-art facilities to students. The community college recently built a new, private LTE network to provide its students with reliable Internet connectivity. The new network was integrated by Kajeet, which implemented the EPC and base stations, and paired them with a variety of user-end devices. This allowed NICC to be able to rapidly deploy its own network during the pandemic and begin to bridge the digital divide. As NICC leaders continued to recognize ongoing challenges their students faced because of their lack of connectivity, they decided it was time to find a solution, but it had to be cost-effective and rapidly deployed to keep classes on schedule. NICC, working with Kajeet, used the existing fiber backhauls and their access to broadband spectrum to build a new, private LTE network. Kajeet installed base stations at each of NICC's campuses and paired them with a variety of user-end devices at students' homes.	Large - county wide.	$85K	*
Colusa	Government	California - CA	Leveraging the B41 spectrum owned by the Office of Education, we assisted the team in building a 4G LTE network spanning 3 of their school districts. The LTE equipment was mounted on water towers, tall structures, and wooden utility poles to provide internet service during the COVID pandemic. Site were linked using wireless Point to Point networks to expand the backhaul capabilities across the county. The sites continue to expand to cover more areas who are underserved by common carriers.	Medium.	$35K	*
City of Birmingham Board of Education	Government	Alabama - AL	Activated, shipped and deployed 10K hotspots and provided data plans for students over the course of 2 years ('22-24')	Large - 10K Hotspots & Data	$1,007,500.00	*
San Bernardino City Unified School District	Education	California - CA	Activated, shipped and deployed 20K hotspots and provided data plans for students over the course of 2 years ('21-current)	Large - 20K Hotspots & Data	$1,528,800.00	*
Pinellas Suncoast Transit Authority	Government	Florida - FL	Provided solution with equipment and wi-fi, with 5G WAN, LAN capabilities for the patrons.	Medium - 175 Units	$753,241.21	*

Table 6: Ability to Sell and Deliver Service

Describe your company's capability to meet the needs of Sourcewell participating entities across the US and Canada, as applicable. Your response should address in detail at least the following areas: locations of your network of sales and service providers, the number of workers (full-time equivalents) involved in each sector, whether these workers are your direct employees (or employees of a third party), and any overlap between the sales and service functions.

Line Item	Question	Response *	
26	Sales force.	Kajeet will leverage its US salesforce to advertise this agreement in its pursuit of Public Sector opportunities for Private Wireless, not limited to State and Local entities, K-12 school districts or higher education. We will target all applicable entities with direct campaigns to make them aware of the agreement and what it offers.	*
27	Dealer network or other distribution methods.	Not applicable.	*
28	Service force.	Kajeet deploys this solution as a managed service, as part of our managed service offering we will provide day 2 support for the network components to support all customers that purchase off this vehicle.	*
29	Describe the ordering process. If orders will be handled by distributors, dealers or others, explain the respective roles of the Proposer and others.	Ordering will be done directly through Kajeet through a dedicated sales representative that would support the customer through the fulfilment process based on the agencies requirements for either a purchase order or other means of contracting.	*
30	Describe in detail the process and procedure of your customer service program, if applicable. Include your response-time capabilities and commitments, as well as any incentives that help your providers meet your stated service goals or promises.	Kajeet Customer Support model is based on ITIL principles. It is a 2 tiered support system. Kajeet Tier 1 Support. Kajeet Tier 1 personnel will be on duty 24 hours a day, seven days a week, including all Kajeet holidays. Tier 1 personnel will triage an Incident and attempt to resolve. Tier 1 personnel will escalate to Tier 2 in the event they are unable to resolve an issue. Kajeet Tier 2 Support. Kajeet provides trained personnel for purposes of providing Tier 2 Support for the Covered Services. All escalations to Kajeet's Tier 2 must originate with Kajeet's Tier 1 team. Kajeet Tier 2 personnel are on duty during business hours, and are on-call to resolve Sev1 and Sev2 incidents. The Customer Support team will response time SLA is 15 minutes of receiving a customer escalation.	*
31	Describe your ability and willingness to provide your products and services to Sourcewell participating entities in the United States.	Kajeet will make this offer available to all Sourcewell participants within the United States.	*
32	Describe your ability and willingness to provide your products and services to Sourcewell participating entities in Canada.	CBRS spectrum is not currently available in Canada so this solution is not applicable but if there is a similar solution or spectrum that becomes available Kajeet reserves the right to review the requirements to support them.	*
33	Identify any geographic areas of the United States or Canada that you will NOT be fully serving through the proposed contract.	Currently we will service the entire United States, as per the previous question today this product is not available in Canada but if it becomes available we will review the requirements.	*
34	Identify any Sourcewell participating entity sectors (i.e., government, education, not-for-profit) that you will NOT be fully serving through the proposed contract. Explain in detail. For example, does your company have only a regional presence, or do other cooperative purchasing contracts limit your ability to promote another contract?	Not applicable.	*
35	Define any specific contract requirements or restrictions that would apply to our participating entities in Hawaii and Alaska and in US Territories.	Not applicable.	*

Table 7: Marketing Plan

Line Item	Question	Response *	

36	Describe your marketing strategy for promoting this contract opportunity. Upload representative samples of your marketing materials (if applicable) in the document upload section of your response.	In coordination with Sourcewell, use various marketing tactics to ensure K-12, Higher Ed and Government entities are aware of Kajeet and Sourcewell's contract, our solutions, value in the market, as well as the contract pricing.
		
		Deliverables:
		- Press Release, as applicable and upon mutual review and agreement
		- Kajeet Website
		  - Create Sourcewell landing page with contract and contact information
		  - Include Sourcewell on the state listing page
		- Provide internal sales team with sales enablement tools
		- Promote contract via digital newsletter to existing customers and prospects
		- Develop informational Social Media posts
		- Placement of Sourcewell logo info on appropriate collateral
		- Sourcewell signage at tradeshows as appropriate
		- Create a Sourcewell-specific sell sheet
		- Participation in conferences and trade shows to promote the Sourcewell contract as appropriate
			*

37	Describe your use of technology and digital data (e.g., social media, metadata usage) to enhance marketing effectiveness.	Extensive use of blog posts, social media, white papers and guides to educate and inform about the industry and wireless solutions. We use metadata to help expand the reach and categorizations of our digital content, for example blogs and web pages.	*
38	In your view, what is Sourcewell's role in promoting contracts arising out of this RFP? How will you integrate a Sourcewell-awarded contract into your sales process?	Kajeet suggests Sourcewell list Kajeet as an awarded/approved vendor on any applicable Sourcewell venues, such as web pages, portals, etc. and assist with a mutually agreed upon Press Release to announce the award/partnership. For conferences and trade shows, provide a placard to display the partnership. Promote via Kajeet provided co-branded collateral in newsletters, and other communication opportunities, as available. Kajeet will train our sales team on the Sourcewell contract terms and conditions, pricing and processes and procedures. A contract will become a Kajeet "Procurement Vehicle" and we will successfully manage and track all orders as we have for other Kajeet-awarded Procurement Vehicles.	*
39	Are your products or services available through an e-procurement ordering process? If so, describe your e-procurement system and how governmental and educational customers have used it.	Not at this time.	*

Table 8: Value-Added Attributes

Line Item	Question	Response *	
40	Describe any product, equipment, maintenance, or operator training programs that you offer to Sourcewell participating entities. Include details, such as whether training is standard or optional, who provides training, and any costs that apply.	Kajeet can provide training resources from the vendors we support (Samsung, Airspan, Cambium, Baicells, and Tarana Wireless). This training can come in the form of instructor-led classes or through courseware available by the vendors. The cost will vary depending on the length of instructor-led classes.	*
41	Describe any technological advances that your proposed products or services offer.	Kajeet utilizes the best of breed technology to deliver state of the art solutions. Our team will review the particular use case and determine the best solution available. Our team provides full turn-key services from design to installation to support. Kajeet offers its own 4G/5G core for RAN-based solutions and offers a proprietary platform called Sentinel for SIM, Device, Subscriber and Network Management.	*
42	Describe any "green" initiatives that relate to your company or to your products or services, and include a list of the certifying agency for each.	The Kajeet Enterprise division is driving positive environmental impact via solutions supporting EV Charging, Telehealth, Remote Workforce, Community Broadband, Autonomous Trucking, and more. By connecting more students, staff, households and workforce Kajeet has supported the fastest increase in Distance Learning, Telehealth, and Teleworking in our nation's history. This has led to a significant reduction in carbon emissions from vehicles and from lower utilization of utilities (HVAC, Electric and more) in facilities across the nation. While these reductions will not be 100% permanent, we are continuing to support the flexibility for students and workers in the future. Kajeet also enables Wi-Fi and other modern technologies on school buses. This has led to reductions in disciplinary incidents on school buses, better service to students and caregivers, and more benefits that will drive student ridership levels. Student ridership of school buses has long been shown to be beneficial to the environment by reducing car-riders, traffic congestion, and emissions – all while providing the safest way for a student to get to school. Additionally, Kajeet is working with school bus manufacturers to build these technologies and benefits into future electric bus platforms to further drive the adoption of electric buses.	*
43	Identify any third-party issued eco-labels, ratings or certifications that your company has received for the equipment or products included in your Proposal related to energy efficiency or conservation, life-cycle design (cradle-to-cradle), or other green/sustainability factors.	Not applicable at this time.	*
44	Describe any Women or Minority Business Entity (WMBE), Small Business Entity (SBE), or veteran owned business certifications that your company or hub partners have obtained. Upload documentation of certification (as applicable) in the document upload section of your response.	Kajeet uses every possible effort to partner with Women, Minority and Small Business entities are part of our deployment strategy. We look for certified partners that can handle components of our deployment in the local areas to ensure local workforce is used when applicable.	*
45	What unique attributes does your company, your products, or your services offer to Sourcewell participating entities? What makes your proposed solutions unique in your industry as it applies to Sourcewell participating entities?	Kajeet is one of the only providers that in the same single pane of glass can service Sourcewell participants with both the Public Wireless service from the Tier 1 operators and the Private Wireless design, installation and management of the network all in the same single pane of glass called Sentinel.	*

Table 9A: Warranty

Describe in detail your manufacturer warranty program, including conditions and requirements to qualify, claims procedure, and overall structure. You may upload representative samples of your warranty materials (if applicable) in the document upload section of your response in addition to responding to the questions below.

Line Item	Question	Response *	
46	Do your warranties cover all products, parts, and labor?	Manufacturer warranty is included in the purchase. Kajeet also offers two Service Management support agreement options that enhances the Manufacturer warranty. For more information on the support agreements see "Sourcewell Support Slide" Attachment.	*
47	Do your warranties impose usage restrictions or other limitations that adversely affect coverage?	No, there is no warranty restrictions for usage.	*
48	Do your warranties cover the expense of technicians' travel time and mileage to perform warranty repairs?	Yes, if a technician is required on site, one will be dispatched.	*
49	Are there any geographic regions of the United States or Canada (as applicable) for which you cannot provide a certified technician to perform warranty repairs? How will Sourcewell participating entities in these regions be provided service for warranty repair?	No, Kajeet provides certified technician support in all regions the Kajeet Private Wireless product is sold. Kajeet support provides a single point of contact for the Sourcewell participating entities to engage for technical assistances. - see "Sourcewell Issue Flow" attachment.	*
50	Will you cover warranty service for items made by other manufacturers that are part of your proposal, or are these warranties issues typically passed on to the original equipment manufacturer?	Kajeet will cover any warranty needs on all equipment purchased from Kajeet. The support team works with manufacturers on warranty requirements.	*
51	What are your proposed exchange and return programs and policies?	The basic return and exchange will be done based on the manufacturer warranty details. If one of the Kajeet support packages is purchased the returns can be as quick as the next business day at no additional cost. See "Sourcewell Support Slide" attachment.	*
52	Describe any service contract options for the items included in your proposal.	Kajeet offers two Support agreement options. Both support options provide a single point of contact for customer support, network & RAN monitoring with customer notifications, vendor management with firmware updates and access to a device management portal. The "Select" provides Monday-Friday 8 to 8 live customer support and standard reverse logistics. The Enterprise option provides 24x7x365 live customer support, with next business day reverse logistics, access to a network status dashboard, and custom SIM (eSIM) management. see "Sourcewell Support Slide" attached.	*

Table 9B: Performance Standards or Guarantees

Describe in detail your performance standards or guarantees, including conditions and requirements to qualify, claims procedure, and overall structure. You may upload representative samples of your performance materials (if applicable) in the document upload section of your response in addition to responding to the questions below.

Line Item	Question	Response *	
53	Describe any performance standards or guarantees that apply to your services	Performance standards for Kajeet's Private LTE Networks are crucial for ensuring reliability and efficient communication within our customers dedicated network environments. Kajeet's standards are defined to meet the expected levels of service quality, reliability, and security that our customer's network requires. Here's a comprehensive list of the performance standards that Kajeet works with their customers on to meet their requirements and expectations: Network Availability Latency Throughput Packet Loss Reliability Coverage Security Interoperability Scalability Quality of Service (QoS) Once these standards are established with our customer, Kajeet implements the Monitoring infrastructure to make these metrics visible to the customer.	*
54	Describe any service standards or guarantees that apply to your services (policies, metrics, KPIs, etc.)	Kajeet's Service standards for Kajeet's Private Networks outline the expected levels of service quality, reliability, and support provided to users and organizations leveraging the customer's network infrastructure. These standards ensure that the customer's network meets the specific needs and requirements of its users, delivering consistent and dependable communication services. Here's a description of service standards applicable to Kajeet's Private Networks: Service Level Agreements (SLAs) Technical Support Maintenance Windows and Updates Capacity Planning Security Measures Service Monitoring and Reporting Disaster Recovery and Continuity Planning Compliance and Regulatory Requirements Customer Satisfaction and Feedback Mechanisms	*

Table 10: Payment Terms and Financing Options

Line Item	Question	Response *	
55	Describe your payment terms and accepted payment methods.	Kajeet typically follows a net 30 day payment terms for the delivery of our services, we prefer electronic funds transfers but can also take checks in the mail.	*
56	Describe any leasing or financing options available for use by educational or governmental entities.	Kajeet has a 3rd party ecosystem that can help customers with financing the networks, this is not a standard offering but they can be brought in to help finance specific deals, these would be non-standard from the terms in this agreement.	*
57	Describe any standard transaction documents that you propose to use in connection with an awarded contract (order forms, terms and conditions, service level agreements, etc.). Upload a sample of each (as applicable) in the document upload section of your response.	Kajeet's standard documents would be network designs, service level agreements and as builds of the network.	*
58	Do you accept the P-card procurement and payment process? If so, is there any additional cost to Sourcewell participating entities for using this process?	No	*

Table 11: Pricing and Delivery

Provide detailed pricing information in the questions that follow below. Keep in mind that reasonable price and product adjustments can be made during the term of an awarded Contract as described in the RFP, the template Contract, and the Sourcewell Price and Product Change Request Form.

Line Item	Question	Response *	
59	Describe your pricing model (e.g., line-item discounts or product-category discounts). Provide detailed pricing data (including standard or list pricing and the Sourcewell discounted price) on all of the items that you want Sourcewell to consider as part of your RFP response. If applicable, provide a SKU for each item in your proposal. Upload your pricing materials (if applicable) in the document upload section of your response.	Line-item discount model based upon manufacturer.	*
60	Quantify the pricing discount represented by the pricing proposal in this response. For example, if the pricing in your response represents a percentage discount from MSRP or list, state the percentage or percentage range.	Our pricing discount varies and is outlined in our equipment pricing table attached	*
61	Describe any quantity or volume discounts or rebate programs that you offer.	We are open to review offering a quantity discount for sizable orders	*
62	Propose a method of facilitating “sourced” products or related services, which may be referred to as “open market” items or “nonstandard options”. For example, you may supply such items “at cost” or “at cost plus a percentage,” or you may supply a quote for each such request.	Our model is cost plus.	*
63	Identify any element of the total cost of acquisition that is NOT included in the pricing submitted with your response. This includes all additional charges associated with a purchase that are not directly identified as freight or shipping charges. For example, list costs for items like pre-delivery inspection, installation, set up, mandatory training, or initial inspection. Identify any parties that impose such costs and their relationship to the Proposer.	Due to the unique nature of each deployment, physical installation pricing would require a site visit or detailed scope of work.	*
64	If freight, delivery, or shipping is an additional cost to the Sourcewell participating entity, describe in detail the complete freight, shipping, and delivery program.	Kajeet pLTE solutions are shipped via prepay and bill. Our common shipment terms are ground service, with air as an option. Term is F.O.B.	*
65	Specifically describe freight, shipping, and delivery terms or programs available for Alaska, Hawaii, Canada, or any offshore delivery.	We have no restrictions from shipping to AK, HI, or Canada.	*
66	Describe any unique distribution and/or delivery methods or options offered in your proposal.	Kajeet offers forward and reverse logistics, warehousing, kitting, and more with Kajeet Concierge - see the attached in "Upload Additional documentation.	*

Table 12: Pricing Offered

Line Item	The Pricing Offered in this Proposal is: *	Comments
67	b. the same as the Proposer typically offers to GPOs, cooperative procurement organizations, or state purchasing departments.	See the pricing table

Table 13: Audit and Administrative Fee

Line Item	Question	Response *	
68	Specifically describe any self-audit process or program that you plan to employ to verify compliance with your proposed Contract with Sourcewell. This process includes ensuring that Sourcewell participating entities obtain the proper pricing, that the Vendor reports all sales under the Contract each quarter, and that the Vendor remits the proper administrative fee to Sourcewell. Provide sufficient detail to support your ability to report quarterly sales to Sourcewell as described in the Contract template.	If awarded, Kajeet recommends a 1.5% administrative fee be remitted to Sourcewell based on the total net value of Sales for which payment has been received. We will track this and submit reports either monthly or quarterly and will make the associated payment to Sourcewell by the 15th day following the submittal of the report. If there are no sales for a particular period, we can provide a no sales/$0 report. Kajeet is willing to create a report or utilize Sourcewell's preferred report. Our price will include the 1.5% administrative fee in the total price based on the total cost of goods and services including installation.	*
69	If you are awarded a contract, provide a few examples of internal metrics that will be tracked to measure whether you are having success with the contract.	Kajeet uses an identifier in Salesforce to capture sales using a particular contract. We will market the contract per our marketing plan and develop strategies to increase sales.	*
70	Identify a proposed administrative fee that you will pay to Sourcewell for facilitating, managing, and promoting the Sourcewell Contract in the event that you are awarded a Contract. This fee is typically calculated as a percentage of Vendor's sales under the Contract or as a per-unit fee; it is not a line-item addition to the Member's cost of goods. (See the RFP and template Contract for additional details.)	Kajeet proposes 1.5% of total sales for which payment has been received.	*

Table 14A: Depth and Breadth of Offered Equipment Products and Services

Line Item	Question	Response *	
71	Provide a detailed description of the equipment, products, and services that you are offering in your proposal.	PTP Unlicensed & PTP Licensed Solutions Kajeet utilizes Cambium Networks to provide these links. They have a robust product set that supports the unlicensed and licensed frequency bands. Our proven Point-to-Point (PTP) series solutions are deployed worldwide, serving highly critical applications in formidable environments for the world's most demanding users. With best-in-class real-world performance and FIPS 140-2 approved security available for government and military applications, the PTP series is your connection to what matters, no matter what. Unlicensed PTP 550 Multicore Gigabit Radio – Performance in the presence of Interference. PTP 550 is a Point to Point Gigabit throughput solution based on 802.11ac Wave 2 operating in 5 GHz wireless space, addressing the gigabit capacity needs for high speed backhaul solutions in short range and middle range applications provides up to 1.36 Gbps throughput with ARQ and asymmetric non-contiguous channel aggregation across 5 GHz band. The PTP 550 solution draws its attributes from Cambium Networks' Point to Point products such as PTP 650/670 and PTP 450i. Each PTP 550 radio is enclosed in a rugged IP66/67 rated metal enclosure, which protects the radio from extreme conditions and solar radiation. PTP 670 Field proven high reliable backhaul for small cell and critical infrastructure. PTP 670 systems provide 4.9 to 6.05 GHz, multi-band flexibility in a single radio and operate in channel sizes from 5 to 45 MHz. PTP 700 PTP 700 is a Point-to-Point wireless broadband solution for mission-critical communications in government, industrial, and public safety spaces. With	

FIPS 140 security and NTIA spectrum certifications, PTP 700 provides models with integrated antennas and/or connectorized for external antennas – allowing for flexible antenna selection at time of deployment. The PTP 700 Beam Steering ODU with integrated Smart Antenna provides electronic beamforming that allows for easy tactical installation and best-in-class interference mitigation in addition to the industry-leading spectral efficiency and processing capabilities of the PTP 700 family of products. PTP 700 supports two different frequency bands. The PTP 45700 covers 4.4 GHz to 5.925 GHz and the PTP 78700 covers 7.125 GHz to 8.5 GHz.

Licensed

PTP 850E Millimeter Wave Radio

PTP 850E E-band Radio, an ultrahigh capacity, all-outdoor Ethernet backhaul operating in the E-band (71–86 GHz). PTP 850E supports 250, 500, 1000, and 2000 MHz channels with BPSK to 512 QAM and delivers up to 10 Gbps capacity in 1+0 configuration. PTP 850E can also be used in multiband configuration with PTP 820C, PTP 820S, or third-party microwave radios to provide robust links of up to 10 Gbps.

The services Kajeet provides for Cambium Network products include RF design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance.

PTMP Unlicensed, PTMP 4G/5G

Kajeet utilizes Cambium Networks to provide these links. Broadband service providers need to provide high throughput internet last-mile access to business and home subscribers in urban, suburban and rural environments. Operators need the ability to cost-effectively deploy point-to-point (PTP) point-to-multipoint (PtMP) fixed wireless access (FWA) networks using 5G, millimeter-wave (mmWave), licensed and unlicensed spectrum. Cambium Networks offers purpose-built point-to-multipoint broadband access solutions using 5G Fixed, PMP 450 (CBRS and unlicensed), ePMP, cnRanger LTE and cnWave millimeter-wave technologies. Network operators can mix and match these technologies to efficiently bridge the digital divide or enable business digital transformation and manage them as ONE Network with a single cloud management system.

PTP 850C Microwave Radio

PTP 850C is next generation all-outdoor, multi-core unit. The PTP 850C has dual-core functionality enabling the system to operate up to 4 Gbps and deliver gigabit-plus capacity.

PTP 820S

PTP 820S, single core radio with All

Outdoor core radio capable of 2048

QAM with ACM

• Support 6-38 GHz

• Support 1+0, 1+1 HSB, 2+0 SP or DP

• Support Advance Frequency reuse

The services Kajeet provides for Cambium Network products include RF design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance.

Millimeter Wave 60 GHz Solutions

Kajeet utilizes Cambium Networks to provide Terragraph certified solutions. The product familiy is called cnWave and is made of Distribution Nodes and

Client Nodes. The cnWave V5000 Distribution Node is featured with two sectors covering up to 280 degrees with beamforming. A single V5000 can connect up to four other distribution nodes or up to 30 client nodes. V5000 can be used for PTP, PMP and mesh configurations. There are several options for clients node based on the speed requirements of the network links.

V1000 - The V1000 Client Node is featured with wide-range, 80º beamforming for easy installation. Powered by 802.3af PoE, V1000 supports up to 2 Gbps with 1 Gbps in the uplink direction and 1 Gbps in the downlink direction.

V2000 - The cnWave 60 GHz V2000 client node features a 2.5 GbE PoE input port as well as a 2.5 GbE PoE 802.3at output port for powering Wi-Fi access points or video surveillance cameras. This makes the V2000 especially well-suited to backhaul Cambium's XV2 series of outdoor Wi-Fi AP's.

V3000 - The V3000 Client Node is featured with a 44.5 dBi high-gain antenna with beamforming. The client nodes can support up to 7.6 Gbps with channel bonding for both PMP and PTP configurations.

The services Kajeet provides for Cambium Network products include RF design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance.

Wi-Fi

Kajeet utilizes Cambium Networks to provide these solutions. Cambium Networks delivers high-performance Wi-Fi to meet the needs of the most demanding enterprises. Give users consistent, "wired-like" performance plus superior coverage and security depending on your needs — whether from single, small office network or global, multi-site enterprise networks. Cambium management solutions offer public cloud, private cloud and on-premises options, all optimized for scalability, zero-touch provisioning and simplified operations. The Wi-Fi solution can be integrated with they other product offerings such as their PMP Solutions (PMP 450 FWA, ePMP FWA, cnRanger LTE, cnWave mmWave, and cnMatrix TX Switches).

Indoor Access Points:

XV2-21X Wi-Fi 6 Indoor Access Point *

The XV2-21X indoor ceiling mount 2×2 Wi-Fi 6 AP offers 2.97 total Gbps of bandwidth. Ideal for hospitality, MDU and small and medium business applications.

XV2-2X Wi-Fi 6 Indoor Access Point

XV2-2X continues the enterprise network convergence with edge-intelligent AP managed by application-intelligent Cambium Networks XMS or cnMaestro™ management system. Choose the management system that best fits your business and use the latest technology from Cambium Networks.

XE3-4 Wi-Fi 6E Indoor Access Point

The XE3-4 is a tri-radio Wi-Fi 6/6E 4×4/2×2 access point (AP) designed to deliver future-proof performance and value for building next generation networks. Wi-Fi 6 delivers faster and more efficient wireless network connections than previous generation Wi-Fi technologies.

XV3-8 Wi-Fi 6 Indoor Access Point

High-density architecture reduces the equipment required while leveraging automation to deliver SLA. XV3-8 includes seamless roaming, fast roaming, automatic RF optimization and interference avoidance to automatically optimize performance to specific local needs. This Software-Defined 8×8 Multi-Radio AP is equipped with dedicated scanning radio and BLE, WPA3 secure public access, Application Control and 802.3bz Ethernet optimized for high density deployments.

XE5-8 Wi-Fi 6E Indoor Access Point

The XE5-8 is a five-radio Wi-Fi 6/6E 8×8/4×4 access point (AP) designed

to deliver high-density, future-proof performance. With five user servicing radios, the XE5-8 delivers the highest density Wi-Fi 6 solution in the industry. Wi-Fi 6E support extends the capacity of Wi-Fi into the 6 GHz band.

Outdoor Access Points:

XV2-23T Wi-Fi 6 Outdoor Access Point

The XV2-23T outdoor 2×2 Wi-Fi 6 AP with long range internal antennas. Ideal for hospitality, education, municipal, transportation and logistics applications.

XV2-2T Wi-Fi 6 Outdoor Access Point

Outdoor Wi-Fi 6 APs with High Efficiency Antennas

Cover significantly larger areas in campus networks and public Wi-Fi hotspot applications. Coupling Wi-Fi 6 technology with high efficiency antennas, the XV2-2T delivers up to 1 km range as well as higher throughput at shorter ranges compared to competitive solutions. Covering more area per AP, network operators can save costs on equipment, cabling, installation, maintenance and access rights for outdoor Wi-Fi deployments. When paired with Cambium Networks' multi-gigabit 60 GHz cnWave solutions for Wi-Fi backhaul, network operators can blanket large areas with blazingly fast speeds – all wirelessly.

XE3-4TN Wi-Fi 6/6E Outdoor Access Point

The XE3-4TN is an outdoor Wi-Fi 6 802.11ax Tri-Radio 4×4/2×2 Access Point with N-type antenna connectors.

The services Kajeet provides for Cambium Network products include RF design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance.

Network Switches

Kajeet utilizes Cambium Networks to provide network switch solutions. They offer a next-gen switching platform offering a cloud-managed, high-performance, enterprise-grade Ethernet switching solution.

The services Kajeet provides for Cambium Network products include Network Design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance.

CBRS Solutions

Kajeet utilizes several manufacturers for supporting a variety of use cases with CBRS.

Airspan Solutions - Kajeet supports all Baicells product lines for indoor and outdoor 4G/5G CBRS solutions. Those products include:

Indoor 4G AirVelocity 1500

Outdoor 4G AirSpeed 1030

Indoor 5G AirVelocity 1901

Outdoor 5G AirSpeed 2900

Baicells Networks - Kajeet supports all of Baicells product lines for indoor and outdoor 4G/5G CBRS solutions. Those products include:

Nova846

Nova436Q

Nova430

		Nova243 Nova227 Neutrino430 Aurora243 Stellar227 Gamma452 Samsung Networks Kajeet supports the CBRS based RAN models supporting 4T4R RRU and 64T64R Massive MIMO radios The services Kajeet provides for these vendor products include Network Design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance. EBS - 2.5 GHz, Band 41 based Solutions Kajeet utilizes several manufacturers for supporting a variety of use cases with EBS Band 41 Baicells Networks - Kajeet supports all of Baicells product lines for indoor and outdoor 4G/5G Band 41 solutions. Those products include: Nova846 Nova246 Nova452 Aurora243 Gamma452 Samsung Networks Kajeet supports the EBS Band 41 based RAN models The services Kajeet provides for these vendor products include Network Design, Equipment Procurement, Installation Services, Onsite & Remote Configuration Services and Solution Support/Maintenance.
72	Describe your supported 911 features and the planning, design, implementation and management products, services and process steps required.	Planning: Needs Assessment: Identify the specific requirements and needs of the community or area where the 911 service will be implemented. Regulatory Compliance: Understand and comply with local, state, and federal regulations governing emergency communication services. Resource Allocation: Determine the budget, personnel, and technology resources required for the project. Risk Assessment: Identify potential risks and challenges associated with implementing and managing the 911 service. Design: System Architecture: Design the overall architecture of the 911 system, including call routing, database management, and user interface. Technology Selection: Choose the appropriate hardware and software technologies to support the 911 service, considering factors like reliability, scalability, and interoperability. User Interface Design: Develop intuitive interfaces for both emergency dispatchers and callers to ensure efficient communication and response. Security Measures: Implement security protocols to protect sensitive information and prevent unauthorized access to the system. Implementation: Infrastructure Setup: Install and configure the necessary hardware and software components of the 911 system. Testing and Quality Assurance: Conduct thorough testing to ensure the reliability and effectiveness of the system under various scenarios. Training: Provide comprehensive training to emergency dispatchers, operators, and other personnel involved in using and managing the 911

service.
Integration: Integrate the 911 system with existing emergency response infrastructure, such as police, fire, and medical services.
Management:
Monitoring and Maintenance: Regularly monitor the performance of the 911 system and perform maintenance to address any issues or updates.
Data Management: Establish protocols for collecting, storing, and analyzing data generated by the 911 system to improve its effectiveness over time.
Continuous Improvement: Implement processes for gathering feedback from users and stakeholders to identify areas for improvement and innovation.
Emergency Response Coordination: Coordinate with other emergency response agencies and organizations to ensure seamless collaboration during emergencies.
Throughout each stage, collaboration between stakeholders such as government agencies, emergency responders, telecommunications providers, and technology vendors are crucial to the success of the 911 service implementation and management. Additionally, adherence to industry standards and best practices can help ensure the reliability, interoperability, and accessibility of the 911 system. *

LPPA stands for "Location Privacy Protection Act." It is a legislative measure aimed at safeguarding the privacy of individuals concerning location data, particularly in the context of emergency services like Enhanced 911 (E911).

In the realm of E911 (Enhanced 911), LPPA may be relevant in the following ways:

Privacy Concerns: With the implementation of E911 services, there is a significant focus on obtaining accurate location information of individuals in emergency situations. However, this raises privacy concerns as location data can be sensitive. LPPA may dictate certain requirements or regulations regarding the collection, use, and sharing of this data to ensure individuals' privacy rights are protected.
Data Handling: E911 systems rely on various technologies to determine a caller's location, such as GPS, Wi-Fi, and cell tower triangulation. LPPA may require strict guidelines on how this location data is handled, stored, and accessed to prevent unauthorized use or disclosure.
Consent and Opt-Out Mechanisms: LPPA may mandate that individuals have the right to provide consent for the collection and use of their location data in E911 services. Additionally, it may require the implementation of mechanisms that allow individuals to opt-out of location tracking when not in an emergency.
Transparency and Accountability: LPPA may require transparency from E911 service providers regarding their data practices, including how location data is collected, used, and shared. It may also necessitate accountability measures to ensure compliance with privacy regulations and the protection of individuals' rights.
Security Measures: In addition to privacy concerns, LPPA may also address security considerations related to the protection of location data from unauthorized access, hacking, or misuse. E911 service providers may be required to implement robust security measures to safeguard this sensitive information.
Overall, LPPA in the context of E911 serves to strike a balance between the critical need for accurate location information in emergency situations and the protection of individuals' privacy rights. It sets forth guidelines and requirements to ensure that location data is handled responsibly and ethically within the framework of emergency services.

Kajeet's networking engineers work with the carriers to ensure that E911 functionality meets all carriers' requirements for E911.

73	Describe your solutions, services, and qualifications, for preventing, mitigating, and responding to private wireless network intrusions and attacks.	Intrusion Detection and Prevention Systems (IDS / IPS): • Kajeet deploys IDS and IPS solutions using industry leading technologies like Crowdstrike tailored to LTE/5G networks to detect malware, file integrity and host intrusion to prevent potential threat vectors before they can even be leveraged. Kajeet still Utilizes the traditional signature-based detection, suspicious activity monitoring, anomaly detection and behavior analysis to identify potential threats but also uses the AI and Machine learning to further protect our infrastructure to prevent bad actors from affecting our operations and customers before they can ever get started. Firewall Solutions: • Kajeet has the ability to Implement firewall solutions capable of inspecting and filtering traffic at the network perimeter to prevent unauthorized access and malicious activities. • This includes the use stateful inspection, application-layer filtering, and intrusion prevention features to enhance security. • Kajeet also has the ability to allow the customer to implement their own firewalls. We integrate customer firewall components with our solution allowing them to implement their policies as needed. Encryption and Authentication: • Kajeet enforces strong encryption protocols (e.g., AES) to secure data in transit over the LTE/5G network, signaling, management traffic, and including the ability to encrypt user data over public networks. • Implement robust authentication mechanisms such as SIM-based authentication, digital certificates, or EAP methods to ensure only authorized devices and users access the network. Access Control Mechanisms: • Kajeet utilizes access control lists (ACLs) and role-based access control (RBAC) to limit network access based on user roles, device types, and locations. • Kajeet implements network segmentation to isolate critical assets and services from potential threats and unauthorized access. Security Monitoring and Logging: • Kajeet deploys security information and event management (SIEM) solutions using industry leading tools including but not limited to DataDog, Thousand Eyes, Pager Duty and ServiceNow to collect, analyze, and correlate security events and logs from various network devices. • Kajeet monitors network traffic, system logs, and user activities to detect and investigate security incidents proactively. Incident Response Services: • Kajeet maintains incident response plans and procedures tailored to private LTE/5G networks, outlining roles, responsibilities, and escalation paths. • Kajeet conducts regular security assessments, penetration testing, and tabletop exercises to validate the effectiveness of security controls and incident response capabilities. • Kajeet maintains a ongoing Vendor Qualifications and Assessment Program: - We choose vendors and service providers with expertise in private LTE/5G networks and cybersecurity. - We Evaluate vendor qualifications, certifications, and track records in delivering secure and reliable solutions for LTE/5G deployments. Regulatory Compliance: • Kajeet is SOC2 type I and II compliance and adheres to NIST and ISO standards for guidelines for controlling our implementations and maintaining best practices. • Kajeet maintains compliance will all state laws and regulatory guidelines where we operate. • Kajeet stays updated on emerging threats, vulnerabilities, and best practices in LTE/5G security to adapt security measures accordingly. By implementing these solutions, leveraging specialized services, and partnering with qualified vendors and organizations Kajeet continues to enhance our security posture of the private LTE/5G networks we deliver. This allows us to effectively prevent, mitigate, and respond to intrusions and attacks keeping our customers safe.
74	For each of the industries listed below (as applicable), describe your understanding of the typical challenges, opportunities, use cases, and solutions for: -Airports -Cities/Governments (local and federal) -Universities/Stadiums -K-12 -Healthcare -Ports/Warehouses -Other	Private wireless networks in airports present both challenges and opportunities due to the complex and dynamic nature of airport operations. Here's an overview of typical challenges, opportunities, use cases, and solutions for private wireless networks in airports: Challenges: High-Density Environments: Airports often experience high densities of passengers, staff, and devices, leading to potential network congestion and performance issues.

Interference: The presence of various wireless technologies, including Wi-Fi, cellular, and aviation communication systems, can cause interference and signal degradation.

Security Concerns: Airports handle sensitive information and require robust security measures to protect against cyber threats, unauthorized access, and data breaches.

Mobility Requirements: Users, devices, and assets in airports are highly mobile, requiring seamless handoff and roaming capabilities across different areas and terminals.

Regulatory Compliance: Airports must comply with aviation regulations, spectrum licensing requirements, and data privacy regulations when deploying private wireless networks.

Opportunities:

Improved Passenger Experience: Private wireless networks can enhance the passenger experience by providing high-speed internet access, real-time flight information, wayfinding services, and personalized services.

Operational Efficiency: Private networks enable airport operators to optimize operations, streamline processes, and improve staff productivity through automation, asset tracking, and data analytics.

Safety and Security Enhancements: Private networks support video surveillance, access control, perimeter security, and emergency communication systems to enhance safety and security in airports.

Revenue Generation: Airports can leverage private networks to offer value-added services, such as location-based advertising, retail promotions, and premium Wi-Fi access, to generate additional revenue streams.

Future-Proofing Infrastructure: Private wireless networks provide flexibility and scalability to accommodate future technology advancements, IoT deployments, and emerging use cases in airports.

Use Cases:

Passenger Wi-Fi Access: Providing high-speed Wi-Fi access to passengers for internet browsing, email, and streaming services.

Baggage Tracking: Using IoT sensors and RFID technology to track the location and status of luggage in real-time.

Facility Management: Monitoring and controlling building systems, HVAC, lighting, and energy usage for improved efficiency and cost savings.

Ground Vehicle Tracking: Tracking and managing ground vehicles, such as baggage carts, vehicles, and maintenance equipment, for operational optimization and safety.

Airport Operations: Enabling staff communication, task management, and workflow automation for airport operations, ground handling, and aircraft servicing.

Solutions:

Carrier-Grade Wi-Fi: Deploying high-capacity Wi-Fi networks with seamless roaming capabilities to provide reliable connectivity throughout the airport.

Private LTE/5G Networks: Implementing private LTE or 5G networks to support mission-critical applications, IoT deployments, and real-time communication services.

IoT Platforms: Leveraging IoT platforms for asset tracking, predictive maintenance, and environmental monitoring to optimize airport operations.

Unified Communications: Deploying unified communications platforms for voice, video, and messaging services to enhance staff collaboration and coordination.

Cybersecurity Solutions: Implementing advanced cybersecurity solutions, such as firewalls, intrusion detection systems, and encryption protocols, to protect

against cyber threats and ensure data privacy.

Cities

Private networks for cities, often referred to as smart city networks, face a range of challenges, opportunities, and use cases, along with various solutions to address them. Here's an overview:

Challenges:

Interoperability: Integrating diverse systems and technologies across various city services and departments can be challenging due to differing protocols and standards.

Data Security and Privacy: With the collection of vast amounts of data from sensors and IoT devices, ensuring data security and protecting citizens' privacy becomes crucial.

Scalability: As cities grow and evolve, the network infrastructure must be scalable to accommodate increasing demands.

Cost and Funding: Building and maintaining a private network infrastructure can be expensive, requiring significant investment.

Legacy Infrastructure: Many cities have legacy systems in place, making it challenging to upgrade to modern technologies seamlessly.

Community Engagement: Ensuring that citizens understand the benefits of smart city initiatives and gaining their trust is essential.

Opportunities:

Efficiency and Optimization: Smart city networks enable the efficient management of resources such as energy, water, and transportation, leading to cost savings and environmental benefits.

Improved Services: Through real-time data collection and analysis, cities can enhance public services such as transportation, waste management, and public safety.

Sustainability: Smart city initiatives can contribute to sustainability goals by reducing energy consumption, greenhouse gas emissions, and traffic congestion.

Economic Development: Implementing smart technologies can attract businesses and talent, stimulating economic growth and innovation.

Quality of Life: By optimizing city services and infrastructure, smart cities can enhance the overall quality of life for residents.

Data-Driven Decision Making: Access to real-time data enables city officials to make informed decisions and respond promptly to emerging issues.

Use Cases:

Traffic Management: Using sensors and cameras to monitor traffic flow and optimize signal timing to reduce congestion.

Public Safety: Deploying surveillance cameras and gunshot detection systems to improve response times and enhance overall safety.

Energy Management: Implementing smart grids and energy-efficient systems to monitor and optimize energy usage.

Waste Management: Using sensors to monitor waste levels in bins and optimize collection routes to reduce costs and environmental impact.

Environmental Monitoring: Deploying sensors to monitor air and water quality, helping to detect pollution and mitigate environmental hazards.

Smart Lighting: Installing smart streetlights that adjust brightness based on ambient light levels and pedestrian activity to save energy.

Solutions:

Integrated Platforms: Deploying platforms that integrate various smart city

applications and services to enable seamless data sharing and interoperability.

Cybersecurity Measures: Implementing robust cybersecurity measures such as encryption, authentication, and access control to protect data and infrastructure.

Cloud Computing: Leveraging cloud-based solutions for data storage, processing, and analytics to scale efficiently and reduce infrastructure costs.

Partnerships and Collaboration: Collaborating with technology vendors, academia, and other stakeholders to develop and deploy smart city solutions.

Community Engagement Programs: Educating and involving citizens in the planning and implementation of smart city initiatives to foster trust and support.

Policy and Regulation: Developing policies and regulations to address data privacy, security, and ethical concerns associated with smart city technologies.

In summary, private networks for cities present a vast array of challenges and opportunities, ranging from technical and logistical hurdles to socioeconomic and environmental benefits. By addressing these challenges and leveraging the opportunities, cities can create more efficient, sustainable, and livable urban environments for their residents.

Government

Private networks for government entities face a unique set of challenges, opportunities, and use cases due to the sensitive nature of government operations and the need for secure, reliable communication. Here's a breakdown of each aspect:

Challenges:

Security: Government networks often handle sensitive information, making them prime targets for cyber threats. Ensuring robust cybersecurity measures to protect against data breaches, hacks, and cyberattacks is paramount.

Regulatory Compliance: Government networks must adhere to strict regulatory standards and compliance requirements, such as those outlined in GDPR, HIPAA, or specific government regulations, adding complexity to network management.

Interoperability: Government agencies often operate in silos with disparate systems and protocols. Ensuring seamless interoperability between different agencies and systems is a challenge.

Resource Constraints: Limited budget and resources can pose challenges in implementing and maintaining robust network infrastructure, especially for smaller government entities.

Scalability: With the increasing volume of data and digital services, government networks must be scalable to accommodate growing demands without compromising performance or security.

Opportunities:

Enhanced Collaboration: Private networks enable secure communication and collaboration among government agencies, fostering better coordination and information sharing.

Efficiency and Productivity: By streamlining processes and enabling automation, private networks can enhance operational efficiency and productivity within government organizations.

Innovation: Private networks provide a platform for adopting emerging technologies such as IoT, AI, and cloud computing, enabling governments to deliver innovative services and solutions.

Citizen Engagement: Secure private networks can facilitate direct engagement with citizens through digital platforms, improving access to government services and information.

Data Analytics: Private networks enable government agencies to collect and analyze vast amounts of data, leading to better decision-making and policy formulation.

Use Cases:

Emergency Services: Private networks support critical communication for emergency response teams, enabling real-time coordination and information sharing during crises.

Smart Cities: Governments can deploy private networks to support smart city initiatives, including traffic management, public safety, and environmental monitoring.

Healthcare: Private networks facilitate secure communication and data exchange within healthcare systems, improving patient care and health outcomes.

Law Enforcement: Private networks support secure communication among law enforcement agencies, enhancing crime prevention and investigation efforts.

E-Government Services: Private networks enable the delivery of online government services, such as tax filing, permit applications, and license renewals, improving accessibility and convenience for citizens.

Solutions:

Secure Networking Infrastructure: Implementing robust encryption, firewalls, intrusion detection/prevention systems, and access controls to safeguard data and communications.

Cloud Services: Leveraging cloud-based solutions for scalability, flexibility, and cost-effectiveness in managing government IT infrastructure and services.

Interoperability Standards: Adopting common standards and protocols to ensure seamless integration and interoperability between different government systems and agencies.

Data Protection and Privacy Measures: Implementing policies and procedures to ensure compliance with data protection regulations and safeguard citizen privacy.

Continuous Monitoring and Updates: Regularly monitoring network activity, conducting security audits, and applying patches and updates to mitigate potential vulnerabilities and security risks.

Private wireless networks in K-12 education settings offer various challenges and opportunities due to the unique requirements of educational institutions, student safety considerations, and the need for reliable connectivity. Here's an overview of typical challenges, opportunities, use cases, and solutions for private wireless networks in K-12 schools: *

Challenges:

Budget Constraints: K-12 schools often have limited budgets for technology infrastructure, including wireless networks, which can impact the selection and deployment of solutions.

Student Safety and Security: Ensuring the safety and security of students and staff members while maintaining appropriate internet access controls and content filtering presents challenges.

Device Management: Managing a diverse array of devices, including laptops, tablets, and smartphones, used by students and faculty members can be complex and resource-intensive.

Digital Equity: Addressing the digital divide by providing equitable access to technology resources and internet connectivity for all students, regardless of socioeconomic background or geographic location.

Compliance with Regulations: Meeting regulatory requirements, such as Children's Internet Protection Act (CIPA) compliance, student data privacy laws (e.g., Family Educational Rights and Privacy Act - FERPA), and state-specific regulations, can be challenging.

Opportunities:

Enhanced Learning Experience: Private wireless networks enable access to digital learning resources, online educational platforms, interactive content, and collaborative tools, enhancing the learning experience for students and teachers.

Personalized Learning: Wireless networks support personalized learning initiatives by enabling adaptive learning applications, student progress tracking, and differentiated instruction based on individual needs and learning styles.

Remote Learning: Private networks facilitate remote learning initiatives, distance education programs, and virtual classrooms, enabling access to educational content and instruction from any location.

STEM Education: Supporting STEM (Science, Technology, Engineering, and Mathematics) education initiatives through access to educational software, programming tools, robotics kits, and online STEM resources.

Parent Engagement: Private wireless networks enable communication platforms, parent portals, and online access to student progress reports, assignments, and school announcements, fostering parental involvement in education.

Use Cases:

Digital Classroom: Integrating wireless technology into classrooms to support interactive whiteboards, digital projectors, student response systems, and online educational content delivery.

1:1 Device Programs: Implementing 1:1 device initiatives, where each student is provided with a laptop or tablet connected to the school's wireless network for personalized learning experiences.

Mobile Learning Labs: Deploying mobile carts equipped with wireless devices, such as laptops or tablets, to facilitate technology-enhanced instruction, collaborative activities, and multimedia projects.

Online Assessments: Conducting online assessments, quizzes, and surveys using wireless devices and secure testing platforms to measure student learning outcomes and progress.

School Safety and Security: Enhancing campus security through wireless surveillance cameras, emergency communication systems, and access control solutions to ensure a safe learning environment.

Solutions:

Wi-Fi Infrastructure: Deploying robust Wi-Fi networks with sufficient coverage and capacity to support high-density areas, such as classrooms, libraries, and common areas.

Content Filtering and Internet Security: Implementing content filtering solutions, firewall appliances, and web security gateways to protect students from accessing inappropriate content and mitigate cybersecurity threats.

Mobile Device Management (MDM): Utilizing MDM platforms to manage and secure mobile devices, enforce usage policies, distribute apps, and track device inventory across the school district.

Educational Software and Platforms: Integrating learning management systems (LMS), educational apps, digital textbooks, and online resources into the curriculum to support teaching and learning objectives.

Parent Communication Tools: Adopting communication platforms, such as parent portals, mobile apps, and automated messaging systems, to facilitate parent-teacher communication, event notifications, and school updates.

Private wireless networks in healthcare settings offer unique challenges and opportunities due to the critical nature of healthcare operations, stringent regulatory requirements, and diverse use cases. Here's an overview of typical challenges, opportunities, use cases, and solutions for private wireless networks in healthcare:

Challenges:

Interference and Reliability: Healthcare environments often have dense deployments of medical equipment, which can cause interference and affect the reliability of wireless networks.

Security and Privacy: Healthcare data is highly sensitive and subject to strict regulatory requirements such as HIPAA (Health Insurance Portability and Accountability Act). Ensuring the security and privacy of patient information is paramount.

Mobility and Coverage: Healthcare professionals require seamless connectivity and coverage across different areas of hospitals, clinics, and medical facilities to access patient records, medical imaging, and communication tools.

Integration Complexity: Integrating wireless networks with existing IT infrastructure, medical devices, electronic health records (EHR) systems, and clinical applications can be complex and require interoperability standards.

Bandwidth and Capacity: The increasing use of bandwidth-intensive applications, such as telemedicine, medical imaging, and video conferencing, requires sufficient network capacity and bandwidth management.

Opportunities:

Improved Patient Care: Private wireless networks enable real-time access to patient records, medical imaging, and diagnostic tools, improving clinical decision-making and patient care outcomes.

Operational Efficiency: Wireless connectivity streamlines workflows, enables remote monitoring of patients, automates administrative tasks, and enhances collaboration among healthcare teams.

Telemedicine and Remote Care: Private networks support telemedicine initiatives, remote patient monitoring, and virtual consultations, extending healthcare services to remote or underserved areas.

IoT and Wearables Integration: Healthcare IoT devices and wearables can collect vital signs, monitor patient activity, and automate data collection, enabling proactive healthcare interventions and chronic disease management.

Data Analytics and Insights: Wireless networks facilitate the collection, analysis, and visualization of healthcare data for clinical research, population health management, and predictive analytics.

Use Cases:

Clinical Mobility: Enabling healthcare professionals to access electronic health records (EHR), medical imaging, and clinical applications securely from mobile devices, tablets, and laptops.

Medical Device Connectivity: Integrating medical devices, such as patient monitors, infusion pumps, and ventilators, with wireless networks for remote monitoring, device management, and alarm notifications.

Asset Tracking and Management: Tracking and managing medical equipment, supplies, and assets using IoT sensors and location-based services to optimize inventory management and reduce equipment loss.

Patient Engagement: Providing patients with wireless access to educational resources, appointment scheduling, telehealth services, and communication tools to enhance patient engagement and satisfaction.

Emergency Response: Supporting emergency communication systems, location tracking, and response coordination during medical emergencies, disasters, and mass casualty incidents.

Solutions:

Wireless Infrastructure: Deploying robust Wi-Fi, Bluetooth, or Zigbee networks tailored to healthcare environments to provide reliable connectivity and seamless roaming.

Mobile Device Management (MDM): Implementing MDM solutions to manage and secure mobile devices, enforce security policies, and ensure compliance

with regulatory requirements.

Secure Access Control: Implementing strong authentication mechanisms, encryption protocols, and access controls to protect patient data and prevent unauthorized access.

Telemedicine Platforms: Deploying telemedicine platforms and video conferencing solutions for remote consultations, virtual visits, and telemonitoring of patients.

Data Analytics Platforms: Leveraging data analytics platforms and business intelligence tools to analyze healthcare data, identify trends, and improve clinical outcomes

Ports/Warehouses

Private networks for ports and warehouses face several challenges and opportunities unique to their environment. Here's an overview:

Challenges:

Coverage and Connectivity: Ports and warehouses often have vast areas with challenging environments for connectivity, such as metal structures or containers. Ensuring seamless coverage throughout the entire area can be difficult.

Security: Ports and warehouses deal with valuable goods and sensitive information. Security breaches can lead to theft, sabotage, or safety hazards. Ensuring data integrity and secure access is paramount.

Interference: With various types of equipment operating in close proximity, there's a risk of interference that can disrupt communications and operations.

Scalability: As operations expand or change, the network must be scalable to accommodate new devices, services, and users without compromising performance.

Integration: Integrating different systems and technologies, such as IoT devices, RFID tags, and inventory management systems, can be complex and require interoperability.

Opportunities:

Efficiency: Private networks can optimize operations by enabling real-time monitoring and control of assets, improving inventory management, and streamlining logistics.

Safety: Enhanced communication capabilities can improve safety measures by enabling rapid response to emergencies, monitoring hazardous materials, and enforcing safety protocols.

Automation: Private networks can support automation initiatives by providing reliable connectivity for autonomous vehicles, drones, and robotic systems, thus increasing productivity and reducing labor costs.

Data Analytics: Collecting data from various sensors and devices within the network enables data-driven decision-making, predictive maintenance, and optimization of processes.

Customization: Tailoring the network to specific operational needs allows for customized solutions that address the unique requirements of ports and warehouses.

Use Cases:

Asset Tracking: Using RFID tags or GPS-enabled devices to track the location and movement of containers, vehicles, and equipment within the port or warehouse.

Remote Monitoring: Monitoring environmental conditions such as temperature, humidity, and air quality in real-time to ensure the integrity of goods and compliance with regulations.

Security Surveillance: Deploying cameras and sensors for video surveillance, intrusion detection, and perimeter security to prevent theft, vandalism, and

		unauthorized access. Predictive Maintenance: Utilizing IoT sensors to monitor equipment health and performance, enabling predictive maintenance to prevent costly downtime and equipment failures. Supply Chain Optimization: Integrating the network with supply chain management systems to optimize inventory levels, streamline workflows, and improve overall efficiency. Solutions: Wireless Technologies: Leveraging technologies like Wi-Fi, Bluetooth, Zigbee, or LoRaWAN for connectivity depending on the specific requirements of coverage, range, and power consumption. Private LTE/5G Networks: Deploying private LTE or 5G networks for high-speed, low-latency communication, especially in environments with high data traffic and mission-critical applications. Edge Computing: Implementing edge computing capabilities to process data closer to the source, reducing latency and bandwidth usage while enhancing security and reliability. Cybersecurity Measures: Implementing encryption, authentication, access control, and intrusion detection systems to safeguard the network and data from cyber threats. Vendor Partnerships: Collaborating with technology vendors and service providers with expertise in industrial IoT, networking, and security to design and deploy tailored solutions. By addressing these challenges and leveraging the opportunities, private networks for ports and warehouses can significantly enhance efficiency, safety, and competitiveness in the logistics industry.	
75	Describe your PWN solutions regarding IoT use cases and associated deployment maturity (ex: conceptual, lab, pilot in-progress, pilot complete, permanent deployment in-progress, permanent deployment fully commissioned, and project closed out). Describe your experience with both simple and complex IoT deployments.	Private Wireless Network (PWN) solutions play a crucial role in enabling various Internet of Things (IoT) use cases due to their reliability, security, and scalability. Here's how PWN solutions can be applied to different IoT use cases and their associated deployment maturity stages: Conceptual Stage: At the conceptual stage, organizations identify potential IoT use cases and evaluate the feasibility of deploying PWN solutions to support them. Use cases might include industrial automation, asset tracking, smart buildings, and environmental monitoring. Deployment maturity: Use cases are still in the planning phase, with no concrete implementation or deployment activities underway. Lab Stage: In the lab stage, organizations conduct proof-of-concept (POC) experiments and testing to validate the technical feasibility and performance of PWN solutions for specific IoT use cases. This stage involves setting up a controlled environment to simulate real-world scenarios and evaluate the interoperability, security, and reliability of PWN infrastructure. Use cases are tested in a laboratory setting to assess their viability and potential challenges. Deployment maturity: POCs are conducted, and initial results are evaluated to determine the next steps for deployment. Pilot In-Progress Stage: At this stage, organizations deploy PWN solutions in a limited-scale pilot environment to test IoT use cases in real-world conditions. Pilot deployments involve integrating PWN infrastructure with IoT devices, sensors, and applications to validate performance, scalability, and user experience.	

Data collection and analysis during the pilot phase help identify and address any technical or operational challenges.

Use cases are actively tested and refined based on feedback and observations from the pilot deployment.

Deployment maturity: Pilot deployments are underway, and organizations are actively gathering insights and making adjustments to optimize performance and functionality.

Pilot Complete Stage:

After successfully completing the pilot phase, organizations move to the pilot complete stage, where the PWN solutions and associated IoT use cases have been thoroughly evaluated and validated.

Lessons learned from the pilot deployment are documented, and any necessary adjustments or enhancements to the PWN infrastructure are implemented.

Stakeholders review the pilot results and make decisions regarding full-scale deployment based on the demonstrated value and ROI of the IoT use cases. *

Deployment maturity: Pilot deployments are concluded, and organizations are preparing for full-scale deployment based on the outcomes and findings.

Permanent Deployment In-Progress Stage:

In this stage, organizations begin the process of deploying PWN solutions and scaling up IoT use cases across broader areas or multiple sites.

Deployment activities include network expansion, device provisioning, configuration, and integration with enterprise systems.

PWN infrastructure is deployed and commissioned for permanent operation, with ongoing monitoring and optimization to ensure reliability and performance.

Use cases transition from pilot to production environments, with gradual rollout and adoption by end-users.

Deployment maturity: Permanent deployment activities are in progress, with PWN solutions being implemented across targeted areas or sites.

Permanent Deployment Fully Commissioned Stage:

At this stage, PWN solutions and associated IoT use cases are fully deployed and operational across all intended locations or areas.

All infrastructure components are commissioned and integrated into the organization's IT ecosystem, with ongoing support and maintenance processes established.

Use cases are in full production mode, delivering value to the organization through improved efficiency, productivity, and operational insights.

Deployment maturity: Permanent deployments are fully completed, and PWN solutions are integrated into day-to-day operations with regular monitoring and management.

Project Closed Out Stage:

The project closed out stage marks the formal conclusion of deployment activities, with all deliverables met, and project objectives achieved.

Final documentation, reports, and performance evaluations are compiled and archived for future reference.

Lessons learned from the deployment process are documented and shared with stakeholders to inform future initiatives.

Ongoing support and maintenance activities transition to standard operations and maintenance procedures.

Deployment maturity: The project is formally closed out, and the focus shifts

		to ongoing operations, monitoring, and optimization of PWN solutions and IoT use cases. Throughout these deployment maturity stages, organizations must engage stakeholders, establish clear objectives, and prioritize security, scalability, and interoperability to ensure the successful implementation of PWN solutions for IoT use cases. Continuous evaluation and adaptation are key to maximizing the value and benefits of PWN deployments in supporting IoT initiatives.	
76	Describe your solutions, services, and best practices for designing and deploying multiple geographically separated sites, as one PWN network (ex: two airports owned and operated by a city, extending enterprise systems) and as separate networks.	Designing and deploying multiple geographically separated sites as one Private Wireless Network (PWN) or as separate networks involves a comprehensive approach that includes solutions, services, and best practices tailored to the specific requirements and objectives of the organization. Here's an overview of the solutions, services, and best practices for each scenario: Multiple Geographically Separated Sites as One PWN Network: Solutions and Services: Unified Network Architecture: Design a unified network architecture that seamlessly connects multiple sites using a common infrastructure and management framework. Private LTE/5G Network: Deploy a private LTE or 5G network across all sites to ensure consistent connectivity, performance, and security. Centralized Management: Implement centralized network management tools and platforms to monitor and control the entire network from a single interface. Redundancy and Failover: Incorporate redundancy and failover mechanisms to ensure high availability and resilience against network disruptions. Security Integration: Integrate robust security measures, such as encryption, authentication, and access control, to protect data and communications across all sites. Best Practices: Site Survey and Planning: Conduct thorough site surveys and planning to optimize network coverage, capacity, and performance across all locations. Standardization: Standardize network equipment, configurations, and protocols to simplify deployment, management, and troubleshooting. Scalability: Design the network to be scalable, allowing for seamless expansion to accommodate future growth and additional sites. Quality of Service (QoS): Implement QoS policies to prioritize critical traffic and ensure consistent performance for latency-sensitive applications. Regular Maintenance and Updates: Establish regular maintenance schedules and procedures to keep the network infrastructure up-to-date and secure. Multiple Geographically Separated Sites as Separate Networks: Solutions and Services: Independent Network Deployments: Deploy separate private LTE or 5G networks at each site, tailored to the specific requirements and characteristics of each location. Site-specific Design: Customize network design and configuration based on the unique characteristics, challenges, and objectives of each site. Local Management: Implement local network management capabilities at each site for granular control and autonomy over network operations. Interconnection: Establish secure interconnections between separate networks, such as VPN tunnels or dedicated links, to facilitate data exchange and collaboration. Compliance and Regulations: Ensure compliance with local regulations and standards governing wireless communications and network operations in each location.	*

		Best Practices: Centralized Oversight: Maintain centralized oversight and governance over all separate networks to ensure consistency, compliance, and alignment with organizational goals. Communication and Collaboration: Foster communication and collaboration between network teams responsible for each site to facilitate knowledge sharing, best practice dissemination, and problem resolution. Performance Monitoring: Implement performance monitoring and reporting mechanisms to track network performance metrics and identify areas for optimization or improvement. Disaster Recovery and Business Continuity: Develop disaster recovery and business continuity plans tailored to each site to mitigate risks and minimize disruptions in the event of network failures or emergencies. Training and Skill Development: Provide training and skill development opportunities for network personnel at each site to enhance their capabilities in network design, deployment, and management. In both scenarios, careful planning, rigorous implementation, and ongoing optimization are essential to ensure the success, reliability, and security of the private wireless networks across multiple geographically separated sites. Collaboration between stakeholders, adherence to best practices, and a focus on scalability and flexibility are key principles to guide the design and deployment process.	
77	Describe your products and services offered for: -Maintaining seamless and continuous connectivity of EUDs -Traversing between PWNs of the same and different PWN manufacturer solutions -Ownership by the same (ex: delivery trucks driving between local, regional, national warehouses) and different Enterprise (ex: aircraft interoperability between airport PWNs)	-Maintaining seamless and continuous connectivity of EUDs Our networks are purpose-built based on the specific use case. The items we consider are density of devices in each area, capacity requirements for those devices, roaming requirements if the area is large, and latency requirements to name a few. Once these are established the RF design is completed and reviewed to ensure that we meet the use case requirements. Our networking and support teams use monitoring tools based on the technology in use to react to outages, reduced connectivity, and other events that impact the end user experience. -Traversing between PWNs of the same and different PWN manufacturer solutions The answer is similar to the above. Kajeet builds networks based on the use case. If roaming between PWNs is a requirement we would ensure that the end user devices support multiple SIM's or eSIM's and that the appropriate PLMN's are registered in each device. As the device moves from one area to another, the device will connect to the adjacent network. -Ownership by the same (ex: delivery trucks driving between local, regional, national warehouses) and different Enterprise (ex: aircraft interoperability between airport PWNs) The is the same scenario addressed above. Devices have to be configured to roam between various networks. An assessment of the providers encountered in a given area would dictate how the devices are configured. We utilize wireless measurement tools that can assist with these surveys as part of the design phase of a project, prior to the deployment phase.	*

78	Describe how your solutions and offerings will support future load-sharing of wireless communications between WiFi, Distributed Antenna Systems (DAS), CBRS, and other communications technologies.	To support future load-sharing of wireless communications between various technologies such as WiFi, Distributed Antenna Systems (DAS), CBRS (Citizens Broadband Radio Service), and others, the following solutions and offerings can be implemented: Software-Defined Networking (SDN): SDN allows for dynamic allocation and optimization of network resources based on real-time traffic patterns and demands. This enables efficient load-sharing between different wireless technologies by intelligently routing traffic and balancing loads across the network. Network Function Virtualization (NFV): NFV decouples network functions from proprietary hardware appliances and virtualizes them, allowing for flexible deployment and scaling of network services. With NFV, different wireless technologies can share resources dynamically, optimizing performance and scalability. Multi-Access Edge Computing (MEC): MEC brings computing resources closer to the edge of the network, enabling localized processing and content delivery. By deploying MEC nodes strategically, different wireless technologies can offload processing tasks to the edge, reducing latency and improving efficiency. Interoperability Standards and APIs: Implementing standardized interfaces and APIs facilitates seamless integration and interoperability between different wireless technologies. This allows for efficient communication and data exchange between WiFi, DAS, CBRS, and other networks, enabling load-sharing and resource optimization. Dynamic Spectrum Sharing (DSS): DSS enables the simultaneous operation of multiple wireless technologies within the same frequency band, dynamically allocating spectrum resources based on demand. This allows for efficient utilization of available spectrum and facilitates load-sharing between different technologies. Quality of Service (QoS) Management: QoS mechanisms prioritize and allocate network resources based on application requirements and user priorities. By implementing QoS policies, network operators can ensure optimal performance for different types of traffic across various wireless technologies, enabling effective load-sharing. Network Analytics and Orchestration: Leveraging network analytics and orchestration platforms allows for real-time monitoring, analysis, and optimization of network performance. By gathering insights into traffic patterns and user behavior, operators can dynamically adjust resource allocation and load-sharing strategies to meet evolving demands. Cross-Technology Coordination: Implementing mechanisms for coordination and cooperation between different wireless technologies enables efficient load-sharing and resource utilization. This includes protocols and algorithms for handover management, spectrum coordination, and traffic offloading between WiFi, DAS, CBRS, and other networks. By deploying these solutions and offerings, organizations can effectively support future load-sharing of wireless communications between WiFi, DAS, CBRS, and other technologies, ensuring efficient resource utilization, improved network performance, and enhanced user experiences.	*
79	Describe how your PWN can operate and be managed as a converged, unified, and integrated extension of other enterprise telecommunications networks and infrastructure solutions (cabled and wireless).	Operating and managing a Private Wireless Network (PWN) as a converged, unified, and integrated extension of other enterprise telecommunications networks and infrastructure solutions involves seamless integration, centralized management, and interoperability across various technologies. Here's how it can be achieved: Interoperability and Standards Compliance:	

Ensure that the PWN infrastructure adheres to industry standards and protocols to facilitate interoperability with existing enterprise telecommunications networks. This includes compatibility with wired (e.g., Ethernet, fiber-optic) and wireless (e.g., WiFi, LTE, 5G) technologies.

Implement protocols and interfaces that enable seamless communication and data exchange between different network components, such as gateways, routers, switches, and access points.

Unified Network Management Platform:

Deploy a centralized network management platform that provides a unified view of the entire telecommunications infrastructure, including both the PWN and other enterprise networks.

This platform should support configuration, monitoring, troubleshooting, and optimization of network resources across wired and wireless domains from a single interface.

Integrate network management tools and systems to streamline operations and improve efficiency in managing the converged infrastructure.

Integration with Enterprise Systems:

Integrate the PWN with existing enterprise systems, such as network management systems (NMS), operations support systems (OSS), and business support systems (BSS).

Enable seamless integration with enterprise applications, databases, and services to support business operations and workflows.

Implement APIs and standard protocols for data exchange and integration with third-party systems, enabling interoperability and automation.

Converged Services and Applications:

Offer converged services and applications that leverage the capabilities of both the PWN and other enterprise networks.

For example, unified communication and collaboration tools can utilize both wired and wireless connectivity options provided by the PWN and other networks to enhance communication efficiency and productivity.

Develop custom applications or service bundles tailored to specific enterprise needs, integrating PWN capabilities with existing enterprise services to deliver value-added solutions.

Security and Compliance:

Implement robust security measures to protect the converged infrastructure from cyber threats and unauthorized access.

Ensure compliance with industry regulations and standards governing data privacy, security, and telecommunications.

Implement security policies, access controls, encryption, and authentication mechanisms to safeguard sensitive data and network resources across the converged infrastructure.

Scalability and Flexibility:

Design the converged infrastructure to be scalable and flexible, capable of accommodating future growth and evolving business requirements.

Employ modular and scalable architecture principles to enable seamless expansion of the PWN and other network components as needed.

Implement dynamic resource allocation and load-balancing mechanisms to optimize performance and utilization across the converged infrastructure.

By operating and managing the PWN as a converged, unified, and integrated extension of other enterprise telecommunications networks and infrastructure solutions, organizations can achieve seamless connectivity, enhanced operational efficiency, and improved agility to meet the evolving demands of modern business environments.

80	Describe your ability to integrate with distributed antenna systems.	Kajeet's offering includes a component of Neutral hosting, which is an alternative to a DAS solution. This offering includes a MOCN gateway that broadcasts the carrier PLMN code to improve coverage inside of the building based on the Private Wireless Network, when deployed there is no reason for a distributed antenna system. *
81	Describe your PWN solutions regarding IoT use cases and associated deployment maturity (ex: conceptual, lab, pilot in-progress, pilot complete, permanent deployment in-progress, permanent deployment fully commissioned, and project closed out).	Private Wireless Network (PWN) solutions play a crucial role in enabling various Internet of Things (IoT) use cases due to their reliability, security, and scalability. Here's how PWN solutions can be applied to different IoT use cases and their associated deployment maturity stages: Conceptual Stage: At the conceptual stage, organizations identify potential IoT use cases and evaluate the feasibility of deploying PWN solutions to support them. Use cases might include industrial automation, asset tracking, smart buildings, and environmental monitoring. Deployment maturity: Use cases are still in the planning phase, with no concrete implementation or deployment activities underway. Lab Stage: In the lab stage, organizations conduct proof-of-concept (POC) experiments and testing to validate the technical feasibility and performance of PWN solutions for specific IoT use cases. This stage involves setting up a controlled environment to simulate real-world scenarios and evaluate the interoperability, security, and reliability of PWN infrastructure. Use cases are tested in a laboratory setting to assess their viability and potential challenges. Deployment maturity: POCs are conducted, and initial results are evaluated to determine the next steps for deployment. Pilot In-Progress Stage: At this stage, organizations deploy PWN solutions in a limited-scale pilot environment to test IoT use cases in real-world conditions. Pilot deployments involve integrating PWN infrastructure with IoT devices, sensors, and applications to validate performance, scalability, and user experience. Data collection and analysis during the pilot phase help identify and address any technical or operational challenges. Use cases are actively tested and refined based on feedback and observations from the pilot deployment. Deployment maturity: Pilot deployments are underway, and organizations are actively gathering insights and making adjustments to optimize performance and functionality. Pilot Complete Stage: After successfully completing the pilot phase, organizations move to the pilot complete stage, where the PWN solutions and associated IoT use cases have been thoroughly evaluated and validated. Lessons learned from the pilot deployment are documented, and any necessary adjustments or enhancements to the PWN infrastructure are implemented. Stakeholders review the pilot results and make decisions regarding full-scale deployment based on the demonstrated value and ROI of the IoT use cases. * Deployment maturity: Pilot deployments are concluded, and organizations are preparing for full-scale deployment based on the outcomes and findings. Permanent Deployment In-Progress Stage: In this stage, organizations begin the process of deploying PWN solutions

		and scaling up IoT use cases across broader areas or multiple sites. Deployment activities include network expansion, device provisioning, configuration, and integration with enterprise systems. PWN infrastructure is deployed and commissioned for permanent operation, with ongoing monitoring and optimization to ensure reliability and performance. Use cases transition from pilot to production environments, with gradual rollout and adoption by end-users. Deployment maturity: Permanent deployment activities are in progress, with PWN solutions being implemented across targeted areas or sites. Permanent Deployment Fully Commissioned Stage: At this stage, PWN solutions and associated IoT use cases are fully deployed and operational across all intended locations or areas. All infrastructure components are commissioned and integrated into the organization's IT ecosystem, with ongoing support and maintenance processes established. Use cases are in full production mode, delivering value to the organization through improved efficiency, productivity, and operational insights. Deployment maturity: Permanent deployments are fully completed, and PWN solutions are integrated into day-to-day operations with regular monitoring and management. Project Closed Out Stage: The project closed out stage marks the formal conclusion of deployment activities, with all deliverables met, and project objectives achieved. Final documentation, reports, and performance evaluations are compiled and archived for future reference. Lessons learned from the deployment process are documented and shared with stakeholders to inform future initiatives. Ongoing support and maintenance activities transition to standard operations and maintenance procedures. Deployment maturity: The project is formally closed out, and the focus shifts to ongoing operations, monitoring, and optimization of PWN solutions and IoT use cases. Throughout these deployment maturity stages, organizations must engage stakeholders, establish clear objectives, and prioritize security, scalability, and interoperability to ensure the successful implementation of PWN solutions for IoT use cases. Continuous evaluation and adaptation are key to maximizing the value and benefits of PWN deployments in supporting IoT initiatives.
82	Describe your approach, process, and timeline for testing and implementing software updates to the PWN.	Implementing software updates to private networks, especially in government settings where security and reliability are paramount, requires a meticulous approach, well-defined processes, and a carefully structured timeline. Here's a step-by-step breakdown of the approach, process, and timeline for testing and implementing software updates: Assessment and Planning: Identify Updates: Determine which software components or systems require updates based on security patches, bug fixes, or feature enhancements. Risk Assessment: Evaluate the potential impact of updates on network stability, security, and functionality. Prioritize updates based on criticality and urgency. Backups: Perform full backups of critical data and configurations to ensure data integrity in case of unexpected issues during the update process. Testing:

Test Environment Setup: Create a testing environment that mirrors the production network as closely as possible.

Functional Testing: Verify that the software updates perform as expected and do not introduce any new bugs or compatibility issues.

Compatibility Testing: Ensure compatibility with existing hardware, software, and third-party integrations.

Security Testing: Assess the impact of updates on network security and conduct vulnerability scans to identify any new security risks.

Performance Testing: Measure the performance impact of updates on network speed, latency, and resource utilization.

Deployment:

Scheduling: Determine an appropriate maintenance window for deploying updates, minimizing disruption to normal network operations.

Rollout Strategy: Decide whether to deploy updates gradually across different segments of the network or all at once.

Monitoring: Continuously monitor the update process to detect any issues or anomalies and ensure a smooth transition.

Fallback Plan: Establish a rollback plan in case the update causes unexpected problems, allowing for a quick return to the previous stable state. *

Communication: Notify stakeholders, including network administrators, end-users, and management, about the update schedule, potential impacts, and any necessary actions they need to take.

Validation and Post-Deployment:

Validation: After deployment, verify that the updates have been successfully applied and that the network is functioning correctly.

User Acceptance Testing (UAT): Engage end-users to validate that the updated software meets their requirements and expectations.

Performance Monitoring: Monitor the network post-update to ensure that performance remains stable and that any issues are promptly addressed.

Documentation: Update documentation, including configuration guides, troubleshooting procedures, and change logs, to reflect the changes made during the update process.

Review and Continuous Improvement:

Post-Implementation Review (PIR): Conduct a review to evaluate the effectiveness of the update process, identify any lessons learned, and make improvements for future updates.

Feedback Loop: Solicit feedback from stakeholders to gather insights into their experience with the updated software and address any remaining issues or concerns.

Patch Management: Establish a proactive patch management strategy to regularly assess, test, and deploy software patches and updates to maintain network security and performance.

Timeline:

The timeline for testing and implementing software updates can vary depending on factors such as the complexity of the updates, the size of the network, and the criticality of the systems being updated.

Generally, the process may take anywhere from days to weeks, with ample time allocated for testing, validation, and post-deployment monitoring.

The timeline should include buffer periods to account for unforeseen complications or delays and ensure a smooth and controlled update process without disrupting ongoing operations.

83	List and describe your various core solution options offered (ex: on-premises, cloud, hybrid, distributed, core services platform) and key differentiators. For each solution, describe the your experience deploying and managing the solution.	Here are some core solution options typically offered for private networks along with their key differentiators and deployment experience: On-Premises Solution: Description: On-premises solutions involve deploying network infrastructure within the organization's physical premises, giving complete control over hardware and software. Key Differentiators: Full control and customization over the network infrastructure. Data sovereignty and compliance adherence can be easily managed. Suitable for organizations with strict security and compliance requirements. Deployment Experience: Deploying on-premises solutions requires careful planning, hardware procurement, installation, and configuration. Organizations need experienced IT staff or external vendors to manage and maintain the infrastructure. Cloud Solution: Description: Cloud solutions involve hosting network services and infrastructure on third-party cloud platforms, providing scalability, flexibility, and cost-effectiveness. Key Differentiators: Scalability: Easily scale resources up or down based on demand. Cost-effectiveness: Pay-as-you-go pricing model reduces upfront costs and allows for better budget management. Accessibility: Accessible from anywhere with an internet connection, promoting remote work and collaboration. Deployment Experience: Deploying a cloud solution involves selecting a cloud provider, provisioning resources, migrating data, and configuring services. Continuous monitoring and management are necessary to optimize performance, security, and cost. Hybrid Solution: Description: Hybrid solutions combine on-premises infrastructure with cloud services, offering the flexibility to leverage both environments based on specific needs. Key Differentiators: Flexibility: Organizations can utilize the scalability of the cloud while retaining control over sensitive data and critical workloads on-premises. Disaster Recovery: Hybrid solutions offer redundancy and disaster recovery options by distributing workloads across on-premises and cloud environments. Compliance: Ideal for organizations with regulatory compliance requirements that necessitate certain data to remain on-premises. Deployment Experience: Deploying a hybrid solution requires integration between on-premises infrastructure and cloud services, often involving hybrid cloud management platforms. Proper planning and configuration are crucial to ensuring seamless operation and data synchronization between environments. Distributed Solution: Description: Distributed solutions involve deploying network resources across multiple locations or edge nodes, bringing services closer to end-users for improved performance and latency. Key Differentiators:	*	

		Low Latency: By distributing resources closer to end-users, distributed solutions reduce latency and improve user experience, critical for real-time applications. Redundancy: Distributed architecture enhances fault tolerance and resilience by avoiding single points of failure. Edge Computing: Enables processing data closer to the source, enhancing efficiency and supporting IoT and AI applications. Deployment Experience: Deploying a distributed solution requires careful planning of edge locations, network connectivity, and workload distribution. Management tools for monitoring and orchestrating distributed resources are essential for effective deployment and ongoing operation. Core Services Platform: Description: Core services platforms provide a comprehensive suite of network services, including security, networking, and management, offered as a unified solution. Key Differentiators: Integration: Core services platforms integrate various network functions into a unified management interface, simplifying deployment, management, and troubleshooting. Security: Built-in security features such as firewall, intrusion detection, and encryption ensure comprehensive protection of network resources and data. Automation: Automation capabilities streamline provisioning, configuration, and maintenance tasks, improving operational efficiency and reducing human error. Deployment Experience: Deploying a core services platform involves selecting a suitable vendor, planning resource allocation, and configuring services according to organizational requirements. Vendor support and training are essential for successful deployment and ongoing management. Overall, the deployment experience varies depending on the specific solution chosen, organizational requirements, and available resources. It's crucial to conduct thorough evaluation and planning to select the most suitable solution and ensure successful implementation and management.
84	Describe your solutions for connecting end user devices that do not natively support PWNs. Note which of your solutions apply to 4G, 5G, and 4G/5G combined networks.	To connect end-user devices that do not natively support Private Wireless Networks (PWNs), several solutions can be employed. Here are some options along with their applicability to 4G, 5G, and 4G/5G combined networks: Virtual Private Network (VPN): Applicability: Suitable for both 4G and 5G networks. Description: VPNs create a secure tunnel between the end-user device and the private network, regardless of the underlying network technology. This enables secure communication and access to resources within the private network. Deployment Experience: VPN solutions are well-established and widely deployed. They are relatively easy to set up and manage, with numerous software and hardware options available. Software-Defined Wide Area Network (SD-WAN): Applicability: Applicable to both 4G and 5G networks. Description: SD-WAN technology abstracts the underlying network infrastructure and allows for centralized management and configuration of network connections. It can provide secure connectivity for end-user devices to access private networks, optimizing performance and reliability. Deployment Experience: SD-WAN solutions require careful planning and configuration but offer flexibility and scalability. They are commonly used in enterprise environments to connect geographically distributed locations.

		Mobile Device Management (MDM) Solutions: Applicability: Relevant for 4G, 5G, and 4G/5G combined networks. Description: MDM solutions enable organizations to remotely manage and configure end-user devices, including those that do not inherently support PWNs. They can enforce security policies, configure VPN connections, and ensure compliance with network requirements. Deployment Experience: MDM solutions are extensively used in various industries for managing fleets of mobile devices. They require integration with device operating systems and may involve some user training for effective deployment. Network Function Virtualization (NFV): Applicability: Suitable for 4G, 5G, and 4G/5G combined networks. Description: NFV decouples network functions from proprietary hardware appliances and virtualizes them, allowing for flexible deployment and scaling of network services. It can be used to instantiate virtualized network functions (VNFs) to support end-user devices' connectivity requirements. Deployment Experience: NFV is gaining traction in telecommunications and enterprise networking environments. Deploying NFV solutions requires expertise in virtualization technologies and network architecture design. Edge Computing and Mobile Edge Computing (MEC): Applicability: Relevant for 5G networks, particularly for ultra-reliable low-latency communication (URLLC) use cases. Description: Edge computing platforms deployed at the edge of the network, including MEC, can host applications and services closer to end-user devices. This can enable secure and low-latency connectivity to private networks, bypassing the need for native support on the devices themselves. Deployment Experience: Edge computing and MEC are still emerging technologies, but they offer promising opportunities for enhancing connectivity and enabling new use cases in 5G networks. Deploying edge computing platforms requires careful consideration of infrastructure and application requirements. These solutions offer diverse approaches to connecting end-user devices to private networks, catering to different deployment scenarios and network technologies. Each option has its own set of advantages and considerations, and the choice depends on factors such as the specific use case, network architecture, security requirements, and scalability needs.	*
85	Describe your mobile edge computing (a.k.a. multi-access edge computing) (MEC) PWN solutions and their key differentiators. For each, describe your experience deploying and managing the solution, as well as associated use cases.	Mobile Edge Computing (MEC), also known as Multi-Access Edge Computing, refers to a network architecture that enables computation and data storage closer to the end-users, typically at the edge of the network. This approach brings several benefits, including reduced latency, improved bandwidth efficiency, and support for low-latency applications. Here are some MEC PWN (Private Wireless Network) solutions and their key differentiators: MEC Deployment with Private 5G Networks: Description: Private 5G networks with MEC capabilities bring ultra-low latency and high bandwidth to support real-time applications and services. MEC servers are deployed at the edge of the private network infrastructure, enabling processing and storage closer to end-users. Key Differentiators: Ultra-Low Latency: MEC reduces latency by processing data closer to end-users, enabling applications such as augmented reality, gaming, and real-time analytics. Bandwidth Optimization: By processing data at the edge, MEC reduces the need to send large volumes of data back and forth to centralized data centers, optimizing bandwidth usage. Enhanced Security: MEC within private 5G networks offers enhanced security features, ensuring data privacy and protection.	

		Experience: Deploying and managing MEC with private 5G networks involves careful planning of network architecture, deployment of MEC servers at edge locations, and integration with existing systems. Experience in network design, security, and application optimization is crucial. Use Cases: Use cases include real-time video analytics, industrial automation, augmented reality/virtual reality (AR/VR) applications, and connected vehicles. MEC Deployment with Private LTE Networks: Description: Private LTE networks can also integrate MEC capabilities to bring low-latency computing closer to end-users. MEC servers are deployed at LTE base stations or edge locations to enable edge computing. Key Differentiators: Low Latency: MEC reduces latency for LTE networks, enabling real-time applications and services. Cost-Effective: Private LTE networks with MEC offer a cost-effective solution for organizations looking to deploy edge computing capabilities without transitioning to 5G. Compatibility: MEC with LTE networks can support legacy devices and applications while still providing the benefits of edge computing. Experience: Deploying MEC with private LTE networks involves integrating MEC servers with existing LTE infrastructure, optimizing network performance, and ensuring compatibility with edge applications. Use Cases: Use cases include smart manufacturing, smart cities, video surveillance, and IoT applications. MEC Deployment with Hybrid Networks (4G/5G): Description: Hybrid networks combining 4G and 5G technologies can leverage MEC to provide edge computing capabilities across different generations of wireless networks. MEC servers are strategically deployed at edge locations to serve both 4G and 5G users. Key Differentiators: Flexibility: Hybrid networks offer flexibility by supporting both 4G and 5G devices and applications, catering to diverse use cases and deployment scenarios. Scalability: MEC in hybrid networks can scale to support varying network demands and user requirements. Future-Proofing: By supporting both 4G and 5G technologies, MEC in hybrid networks ensures readiness for future network transitions. Experience: Deploying MEC in hybrid networks requires expertise in integrating MEC servers with both 4G and 5G infrastructure, optimizing network performance, and managing interoperability between different network generations. Use Cases: Use cases include public safety, enterprise networking, IoT applications, and mobile broadband services. In deploying and managing MEC solutions, considerations include network architecture design, edge server deployment, application optimization, security, and ongoing monitoring and maintenance. Use cases span various industries, including telecommunications, manufacturing, healthcare, transportation, and entertainment, among others.	*

Table 14B: Depth and Breadth of Offered Equipment Products and Services

Indicate below if the listed types of equipment, products, and services are offered within your proposal. Provide an additional explanation in the text box provided, as necessary.

Line Item	Category or Type	Offered *	Comments
86	Assessment and strategy	(•) Yes ( ) No	Define Objectives and Requirements: Identify the primary objectives of implementing a private wireless network, such as improving connectivity, enhancing security, enabling mobility, or supporting specific applications. Define the requirements for the network, including coverage area, capacity, performance metrics (e.g., latency, throughput), security protocols, regulatory compliance, and budget constraints. Assess Current Infrastructure and Capabilities: Evaluate existing network infrastructure, including wired and wireless networks, IT systems, and operational processes. Assess organizational capabilities, including technical expertise, staffing resources, budget allocation, and vendor relationships. Understand Use Cases and Applications: Identify the use cases and applications that will drive the deployment of the private wireless network. Determine the specific requirements of each use case, such as data bandwidth, latency sensitivity, device mobility, and security considerations. Evaluate Spectrum and Licensing Options: Assess the availability of spectrum bands suitable for private wireless networks, such as licensed, unlicensed, or shared spectrum. Investigate regulatory requirements and licensing options for acquiring spectrum allocations, if applicable. Identify Technology Solutions: Explore available technology solutions for implementing the private wireless network, including Wi-Fi, LTE, 5G, or other emerging wireless technologies. Evaluate the advantages, limitations, and suitability of each technology option based on the identified requirements and use cases. Risk Assessment and Mitigation: Conduct a risk assessment to identify potential threats, vulnerabilities, and challenges associated with deploying a private wireless network. Develop risk mitigation strategies to address security risks, operational disruptions, regulatory compliance issues, and other potential concerns. Cost-Benefit Analysis: Perform a cost-benefit analysis to assess the financial implications of deploying a private wireless network. Evaluate the upfront costs of equipment acquisition, installation, and licensing, as well as ongoing operational expenses, maintenance costs, and potential return on investment (ROI). Develop Deployment Strategy: Define a deployment strategy outlining the phased approach for deploying the private wireless network.

			Determine deployment timelines, milestones, resource requirements, and roles and responsibilities of stakeholders involved in the deployment process. Plan for Integration and Interoperability: Identify integration points with existing IT systems, network infrastructure, and operational processes to ensure seamless interoperability and compatibility. Develop integration plans, testing procedures, and migration strategies to minimize disruptions and ensure smooth transition to the new network environment. Continuous Improvement and Optimization: Establish mechanisms for ongoing monitoring, performance measurement, and optimization of the private wireless network. Implement feedback loops, performance metrics, and Key Performance Indicators (KPIs) to track progress, identify areas for improvement, and adapt strategies accordingly.
87	Network design, migration, and deployment, including network configuration and Spectrum Access System (SAS) registration	(•) Yes ( ) No	Kajeet's Private Network Engineers are experienced in Designing, migrating, and deploying a Private Wireless Network involves several key steps to ensure that the network meets the specific needs of the organization, provides reliable connectivity, and maintains high levels of security. Here's an overview of the process, including a network configuration overview: Assessment and Requirements Gathering Identify the customer's requirements, including coverage area, capacity, performance expectations, security requirements, and regulatory compliance. Assess existing network infrastructure, including legacy systems and equipment, to determine compatibility and migration strategies. Network Design and Architecture Develop a network architecture that meets the identified requirements, considering factors such as topology, scalability, redundancy, and fault tolerance. Determine the appropriate wireless technologies and standards for the deployment, such as Wi-Fi, LTE, or 5G, based on coverage area, bandwidth requirements, and application needs. Spectrum and Frequency Planning: • Allocate spectrum and frequencies for the Private Wireless Network, considering available licensed and unlicensed bands, regulatory constraints, and interference mitigation strategies. • Optimize frequency assignments and channel allocations to minimize co-channel interference and maximize spectral efficiency.

			Spectrum Access System (SAS) Registration Kajeet has on staff multiple OnGo CPI Certified engineers on Staff that process Spectrum Access System (SAS) registration on behalf of our customers. The Spectrum Access System (SAS) registration process involves several steps to enable entities to gain access to the Citizens Broadband Radio Service (CBRS) spectrum band in the United States. Here's an overview of the SAS registration process: Determine Eligibility: Ensure that your organization meets the eligibility requirements to register with a SAS provider. Eligible entities may include wireless carriers, internet service providers, enterprise networks, and other organizations seeking to deploy or utilize CBRS-enabled devices and services. Select SAS Provider: Assist in choosing a SAS provider from the list of authorized SAS administrators approved by the Federal Communications Commission (FCC). SAS providers are responsible for managing access to the CBRS spectrum band and ensuring interference mitigation among different users. Submit Registration Application: Contact the chosen SAS provider to initiate the registration process. Submit the required application forms, along with any supporting documentation or information requested by the SAS provider. Provide Required Information: Provide accurate and detailed information about your organization, including company name, contact information, FCC Registration Number (FRN), physical address, and legal representative details. You may also need to provide technical specifications of the devices or systems you intend to deploy in the CBRS band. Complete Background Checks: Some SAS providers may conduct background checks or verification procedures to validate the information provided in the registration application. Ensure that all information provided is accurate and up-to-date to expedite the registration process. Sign Agreements: Review and sign any necessary agreements or contracts with the SAS provider, outlining the terms and conditions of spectrum access, usage rights, compliance obligations, and dispute resolution mechanisms. Pay Fees (if applicable): Some SAS providers may charge registration or access fees for utilizing their services. Ensure that you understand the fee structure and payment terms associated with accessing the CBRS spectrum through the selected SAS provider. Receive Approval: Upon successful completion of the registration process and verification by the SAS provider, you will receive approval to access the CBRS spectrum band. The SAS provider may issue a unique identifier or credential that allows your organization to operate CBRS-enabled devices or systems within the authorized spectrum range. Comply with Regulations: Ensure ongoing compliance with FCC regulations, SAS provider requirements, and CBRS operational rules governing spectrum access, usage, and interference management. Maintain accurate records, adhere to reporting obligations, and cooperate with regulatory authorities as necessary. Renew Registration (if required): Monitor registration expiration dates and renew your registration with the SAS provider as needed to maintain uninterrupted access to the CBRS spectrum band. Stay informed about regulatory	*

			updates, policy changes, and best practices for spectrum management and utilization. Equipment Selection and Procurement: Select and procure the necessary hardware and equipment for the deployment, including access points, base stations, antennas, routers, switches, and security appliances. Ensure compatibility, interoperability, and support for the chosen network architecture and technologies. Network Configuration: Configure network devices, including access points, routers, switches, and security appliances, according to the design specifications and best practices. Configure wireless parameters such as SSIDs, security protocols (WPA2, WPA3), encryption keys, VLANs, and Quality of Service (QoS) policies to optimize performance and security. Security Implementation: Implement robust security measures to protect the Private Wireless Network from unauthorized access, cyber threats, and data breaches. Configure access controls, authentication mechanisms, encryption protocols, firewall rules, and intrusion detection/prevention systems to safeguard network assets and user data. Testing and Validation: Conduct thorough testing and validation of the Private Wireless Network before deployment to ensure proper functionality, performance, and security. Perform site surveys, signal propagation tests, throughput measurements, and security audits to identify and resolve any issues or deficiencies. Migration and Deployment: Develop a deployment plan outlining timelines, resources, and procedures for migrating to the new Private Wireless Network. Deploy network infrastructure, including access points, base stations, and network devices, according to the deployment plan and design specifications. Coordinate with stakeholders, IT personnel, and end-users to minimize disruptions and ensure a smooth transition to the new network environment. Monitoring and Maintenance: Implement network monitoring tools and systems to monitor performance, availability, and security of the Private Wireless Network. Establish procedures for ongoing maintenance, software updates, firmware upgrades, and troubleshooting to address any issues or vulnerabilities proactively. Documentation and Training: Document network configurations, design specifications, deployment procedures, and troubleshooting guidelines for reference and future maintenance. Provide training and support to IT staff, network administrators, and end-users to ensure effective operation	

			and utilization of the Private Wireless Network.	
88	Acquisition and installation of needed equipment to support the private wireless network	(•) Yes ( ) No	Acquiring and installing the necessary equipment to support a private wireless network involves several steps to ensure that the network infrastructure is properly deployed, configured, and integrated. Here's an overview of the process: Equipment Assessment and Planning: Identify the required equipment based on the network design and architecture, including access points, base stations, routers, switches, antennas, cables, and other network components. Determine the quantity, specifications, and compatibility requirements of each equipment type based on coverage area, capacity, performance objectives, and application needs. Vendor Selection and Procurement: Research and evaluate potential vendors, manufacturers, and suppliers of network equipment based on factors such as product quality, reliability, support services, pricing, and availability. Obtain quotes, proposals, and product specifications from selected vendors to compare options and make informed purchasing decisions. Equipment Purchase and Delivery: Place orders for the selected network equipment with the chosen vendors or suppliers, ensuring compliance with procurement policies, budget constraints, and delivery timelines. Coordinate with vendors to schedule equipment delivery, logistics, and shipping arrangements to ensure timely receipt and availability of the necessary hardware and components. Site Preparation: Prepare the installation sites for the deployment of network equipment, including access points, base stations, antennas, and associated infrastructure. Ensure that site locations comply with regulatory requirements, safety standards, and environmental considerations, such as access permissions, zoning regulations, and power supply availability. Installation and Deployment: Deploy and install the network equipment according to the network design and deployment plan, following manufacturer guidelines, installation instructions, and best practices. Mount access points, base stations, antennas, and other hardware at designated locations, ensuring proper alignment, orientation, and coverage patterns to optimize signal propagation and coverage. Configuration and Integration: Configure and provision the installed equipment with the necessary settings, parameters, and network configurations to establish connectivity, interoperability, and functionality. Integrate the network equipment with existing infrastructure, IT systems, and operational workflows, ensuring seamless interoperability and compatibility with deployed applications and services. Testing and Commissioning:	*

			Conduct comprehensive testing and validation of the installed equipment to verify proper functionality, performance, and compliance with design specifications and operational requirements. Perform site surveys, signal measurements, connectivity tests, and system checks to identify and address any issues, defects, or performance bottlenecks. Training and Documentation: Provide training and support to network administrators, IT staff, and end-users on the operation, management, and maintenance of the installed equipment. Document installation procedures, configuration settings, equipment inventory, and maintenance guidelines for reference, troubleshooting, and future upgrades. Quality Assurance and Compliance: Ensure that the installation and deployment of network equipment comply with industry standards, regulatory requirements, and vendor guidelines for safety, performance, and reliability. Conduct quality assurance checks, audits, and inspections to verify compliance with installation standards and best practices. Maintenance and Support: Establish procedures for ongoing maintenance, monitoring, and support to ensure the continued operation and performance of the installed equipment. Implement preventive maintenance measures, software updates, and periodic inspections to detect and address potential issues proactively. By following these steps, organizations can effectively acquire and install the necessary equipment to support a private wireless network, ensuring reliable connectivity, optimal performance, and seamless integration with existing infrastructure and operations. Collaboration between cross-functional teams, adherence to best practices, and diligent project management are essential for successful equipment acquisition and deployment.
89	Ongoing operations, maintenance, planning, expansion, and upgrading of the private wireless network and related components	(•) Yes ( ) No	Ongoing operations, maintenance, planning, expansion, and upgrading of a private wireless network and its related components are critical to ensuring its continued reliability, performance, and alignment with evolving business needs. Here's an overview of each aspect: Operations: Regularly monitor network performance, availability, and security to identify any issues or abnormalities. Establish procedures for incident management, troubleshooting, and resolution to minimize downtime and disruptions. Conduct routine network health checks, audits, and performance assessments to ensure optimal operation. Provide ongoing support and assistance to end-users, network administrators, and IT staff to address any operational issues or concerns. Maintenance: Implement preventive maintenance measures to proactively identify and address potential issues before they escalate.

			Schedule regular inspections, software updates, firmware upgrades, and hardware replacements to maintain the health and reliability of network components. Document maintenance activities, update asset inventories, and track service history for all network equipment and infrastructure. Collaborate with vendors, service providers, and maintenance contractors to ensure timely and effective maintenance support. Planning: Continuously assess business requirements, technology trends, and industry developments to inform strategic planning and decision-making. Develop long-term roadmaps and investment plans for network expansion, modernization, and optimization. Conduct capacity planning and resource forecasting to anticipate future demand and scalability needs. Engage stakeholders, management, and technical experts in the planning process to align network objectives with organizational goals and priorities. Expansion: Identify opportunities for network expansion, coverage enhancement, and service extension to support business growth and emerging use cases. Evaluate potential deployment locations, frequency allocations, and spectrum availability for new network infrastructure. Coordinate with regulatory authorities, landlords, and property owners to secure permits, licenses, and access rights for expansion projects. Deploy additional equipment, access points, or base stations as needed to expand network coverage and capacity. Upgrading: Stay informed about technological advancements, standards updates, and product innovations relevant to the private wireless network. Evaluate the feasibility and benefits of upgrading network components, software platforms, and communication protocols to leverage new features, improve performance, and enhance security. Develop upgrade plans, migration strategies, and testing procedures to minimize disruption and ensure seamless transition to upgraded systems. Allocate resources, budget, and timelines for upgrading critical network infrastructure components, such as core network elements, radio access equipment, and security systems. By prioritizing ongoing operations, maintenance, planning, expansion, and upgrading activities, organizations can ensure the long-term success and sustainability of their private wireless networks. Proactive management, strategic investments, and continuous improvement initiatives are essential for adapting to changing business requirements, technological advancements, and market dynamics.	*
90	Related network component solutions, such as private wireless network (PWN) cores, SIMs, radio access networks (RANs), gateways, end	(•) Yes ( ) No	Ongoing operations, maintenance, planning, expansion, and upgrading of a private wireless network and its related components are critical to ensuring its continued reliability,	

	user devices (EUDs), network management tools, and products		performance, and alignment with evolving business needs. Here's an overview of each aspect: Operations: Regularly monitor network performance, availability, and security to identify any issues or abnormalities. Establish procedures for incident management, troubleshooting, and resolution to minimize downtime and disruptions. Conduct routine network health checks, audits, and performance assessments to ensure optimal operation. Provide ongoing support and assistance to end-users, network administrators, and IT staff to address any operational issues or concerns. Maintenance: Implement preventive maintenance measures to proactively identify and address potential issues before they escalate. Schedule regular inspections, software updates, firmware upgrades, and hardware replacements to maintain the health and reliability of network components. Document maintenance activities, update asset inventories, and track service history for all network equipment and infrastructure. Collaborate with vendors, service providers, and maintenance contractors to ensure timely and effective maintenance support. Planning: Continuously assess business requirements, technology trends, and industry developments to inform strategic planning and decision-making. Develop long-term roadmaps and investment plans for network expansion, modernization, and optimization. Conduct capacity planning and resource forecasting to anticipate future demand and scalability needs. Engage stakeholders, management, and technical experts in the planning process to align network objectives with organizational goals and priorities. Expansion: Identify opportunities for network expansion, coverage enhancement, and service extension to support business growth and emerging use cases. Evaluate potential deployment locations, frequency allocations, and spectrum availability for new network infrastructure. Coordinate with regulatory authorities, landlords, and property owners to secure permits, licenses, and access rights for expansion projects. Deploy additional equipment, access points, or base stations as needed to expand network coverage and capacity. Upgrading: Stay informed about technological advancements, standards updates, and product innovations relevant to the private wireless network. Evaluate the feasibility and benefits of upgrading network		

			components, software platforms, and communication protocols to leverage new features, improve performance, and enhance security. Develop upgrade plans, migration strategies, and testing procedures to minimize disruption and ensure seamless transition to upgraded systems. Allocate resources, budget, and timelines for upgrading critical network infrastructure components, such as core network elements, radio access equipment, and security systems. By prioritizing ongoing operations, maintenance, planning, expansion, and upgrading activities, organizations can ensure the long-term success and sustainability of their private wireless networks. Proactive management, strategic investments, and continuous improvement initiatives are essential for adapting to changing business requirements, technological advancements, and market dynamics.	

Table 14C: Depth and Breadth of Offered Equipment Products and Services

Indicate below if the listed types of equipment, products, and services are offered within your proposal. Provide an additional explanation in the text box provided, as necessary.

Line Item	Category	Product/Service	Offered	Explain *	
91	System Features and Capabilities:		(•) Yes ( ) No	Please see below answers.	
92		Multi-tenant support (network segmentation/slicing)	(•) Yes ( ) No	Kajeet's offering provides a multi-tenant offering via network segmentation and slicing.	*
93		Roaming from: Private-to-public networks Public-to-private networks Private-to-private networks	(•) Yes ( ) No	Kajeet can roam from private to public, public to private, and private to private, this requires dual sim capability.	*
94		Performance monitoring	(•) Yes ( ) No	Kajeet provides a fully managed service that includes performance monitoring of the network.	*
95		Multi-network roaming	(•) Yes ( ) No	See 93.	*
96		Radio site capacity	(•) Yes ( ) No	Radio site capacity is dependent on the design of the network, each design is customized based on requirements that are received from the customer during the intake process before the network design being started.	*
97		Bandwidth and throughput	(•) Yes ( ) No	Bandwidth and throughput is dependent on the design of the network, each design is customized based on requirements that are received from the customer during the intake process before the network design being started.	*
98		Mode (4G only, 4G to 5G Upgrade, 4/5G mixed mode, 5G only)	(•) Yes ( ) No	Kajeet supports both 4G and 5G.	*
99		Quality of Service (QoS)	(•) Yes ( ) No	Kajeet can offer QoS (Quality of Service) through it's management platform that it provides its customers.	*
100		Network Slicing	(•) Yes ( ) No	Kajeet offers Network slicing as part of it's CORE offering.	*
101	Network Components:		(•) Yes ( ) No	See below.	
102		High Availability	(•) Yes ( ) No	Kajeet has a high availability CORE offering.	*
103		Indoor RAN	(•) Yes ( ) No	Kajeet supports Indoor RAN from multiple manufacturers.	*
104		Outdoor RAN	(•) Yes ( ) No	Kajeet supports Outdoor RAN from multiple manufacturers.	*

105		Open/proprietary RAN	(•) Yes ( ) No	Kajeet is RAN agnostic.	*
106		Open/proprietary Core	(•) Yes ( ) No	Kajeet has developed a Core based on the ONF (Open Networking Foundation) platform called Aether. This is an open-source Core that can develop on.	*
107		SIMs	(•) Yes ( ) No	Kajeet has both physical and eSIM capability for its services.	*
108		End User Devices	(•) Yes ( ) No	Kajeet can provide end-user devices (CPEs), we have a wide range of compatible CPEs based on customer requirements.	*
109		Gateways	(•) Yes ( ) No	Please refer to 108.	*
110	Design and Installation Services:		(•) Yes ( ) No	Kajeet provides a fully managed service that includes the design, installation, testing, maintenance, and monitoring of the network after installation.	
111		RF Design	(•) Yes ( ) No	Please refer to 110.	*
112		System Design	(•) Yes ( ) No	Please refer to 110.	*
113		Radio Installation	(•) Yes ( ) No	Please refer to 110.	*
114		Core Installation	(•) Yes ( ) No	Please refer to 110.	*
115		System integration and testing	(•) Yes ( ) No	Please refer to 110.	*
116		Application integration support	(•) Yes ( ) No	Kajeet can support application integration, we have an open set of API's that allows applications to be integrated into the solution.	*
117		Network slicing	(•) Yes ( ) No	Kajeet supports network slicing as part of its Core offering.	*
118		Operations, Maintenance and Administrative Services:	(•) Yes ( ) No	Please refer to 110.	
119		Spectrum Access System	(•) Yes ( ) No	Kajeet has access to SAS (Spectrum Acces System), we work with both Google and Federated to support SAS services.	
120		Network monitoring	(•) Yes ( ) No	Please refer to 110.	

Table 15: Exceptions to Terms, Conditions, or Specifications Form

Line Item 121. **NOTICE**: To identify any exception, or to request any modification, to Sourcewell standard Contract terms, conditions, or specifications, a Proposer must submit the proposed exception(s) or requested modification(s) via redline in the Contract Template provided in the "Bid Documents" section. Proposer must upload the redline in the "Requested Exceptions" upload field. All exceptions and/or proposed modifications are subject to review and approval by Sourcewell and will not automatically be included in the Contract.

Do you have exceptions or modifications to propose?	Acknowledgement *
	( ) Yes (•) No

Documents

Ensure your submission document(s) conforms to the following:

1. Documents in PDF format are preferred. Documents in Word, Excel, or compatible formats may also be provided.

2. Documents should NOT have a security password, as Sourcewell may not be able to open the file. It is your sole responsibility to ensure that the uploaded document(s) are not either defective, corrupted or blank and that the documents can be opened and viewed by Sourcewell.

3. Sourcewell may reject any response where any document(s) cannot be opened and viewed by Sourcewell.

4. If you need to upload more than one (1) document for a single item, you should combine the documents into one zipped file. If the zipped file contains more than one (1) document, ensure each document is named, in relation to the submission format item responding to. For example, if responding to the Marketing Plan category save the document as "Marketing Plan."

- Pricing - 240220 Kajeet Catalog 2024_SOurcewell Final submission.xlsx - Tuesday February 20, 2024 15:15:03
- Financial Strength and Stability (optional)
- Marketing Plan/Samples - 240220 Airspan_Reseller Authorization letter for Sourcewell RFP.pdf - Tuesday February 20, 2024 15:21:43
- WMBE/MBE/SBE or Related Certificates - 240220 Baicells Authorized Reseller Certificate for Kajeet.pdf - Tuesday February 20, 2024 15:20:55
- Warranty Information - Sourcewell Support Docs.pptx - Thursday February 15, 2024 15:41:59
- Standard Transaction Document Samples (optional)
- Requested Exceptions (optional)
- Upload Additional Document - 240220 Kajeet Conierge RFP Response_Sourcewell.pptx - Sunday February 18, 2024 17:05:24

Addenda, Terms and Conditions

PROPOSER AFFIDAVIT AND ASSURANCE OF COMPLIANCE

I certify that I am the authorized representative of the Proposer submitting the foregoing Proposal with the legal authority to bind the Proposer to this Affidavit and Assurance of Compliance:

1. The Proposer is submitting this Proposal under its full and complete legal name, and the Proposer legally exists in good standing in the jurisdiction of its residence.

2. The Proposer warrants that the information provided in this Proposal is true, correct, and reliable for purposes of evaluation for contract award.

3. The Proposer, including any person assisting with the creation of this Proposal, has arrived at this Proposal independently and the Proposal has been created without colluding with any other person, company, or parties that have or will submit a proposal under this solicitation; and the Proposal has in all respects been created fairly without any fraud or dishonesty. The Proposer has not directly or indirectly entered into any agreement or arrangement with any person or business in an effort to influence any part of this solicitation or operations of a resulting contract; and the Proposer has not taken any action in restraint of free trade or competitiveness in connection with this solicitation. Additionally, if Proposer has worked with a consultant on the Proposal, the consultant (an individual or a company) has not assisted any other entity that has submitted or will submit a proposal for this solicitation.

4. To the best of its knowledge and belief, and except as otherwise disclosed in the Proposal, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest. An organizational conflict of interest exists when a vendor has an unfair competitive advantage or the vendor's objectivity in performing the contract is, or might be, impaired.

5. The contents of the Proposal have not been communicated by the Proposer or its employees or agents to any person not an employee or legally authorized agent of the Proposer and will not be communicated to any such persons prior to Due Date of this solicitation.

6. If awarded a contract, the Proposer will provide to Sourcewell Participating Entities the equipment, products, and services in accordance with the terms, conditions, and scope of a resulting contract.

7. The Proposer possesses, or will possess before delivering any equipment, products, or services, all applicable licenses or certifications necessary to deliver such equipment, products, or services under any resulting contract.

8. The Proposer agrees to deliver equipment, products, and services through valid contracts, purchase orders, or means that are acceptable to Sourcewell Members. Unless otherwise agreed to, the Proposer must provide only new and first-quality products and related services to Sourcewell Members under an awarded Contract.

9. The Proposer will comply with all applicable provisions of federal, state, and local laws, regulations, rules, and orders.

10. The Proposer understands that Sourcewell will reject RFP proposals that are marked "confidential" (or "nonpublic," etc.), either substantially or in their entirety. Under Minnesota Statutes Section 13.591, subdivision 4, all proposals are considered nonpublic data until the evaluation is complete and a Contract is awarded. At that point, proposals become public data. Minnesota Statutes Section 13.37 permits only certain narrowly defined data to be considered a "trade secret," and thus nonpublic data under Minnesota's Data Practices Act.

11. Proposer its employees, agents, and subcontractors are not:
    1. Included on the "Specially Designated Nationals and Blocked Persons" list maintained by the Office of Foreign Assets Control of the United States Department of the Treasury found at: https://www.treasury.gov/ofac/downloads/sdnlist.pdf;

    2. Included on the government-wide exclusions lists in the United States System for Award Management found at: https://sam.gov/SAM/; or

    3. Presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from programs operated

by the State of Minnesota; the United States federal government or the Canadian government, as applicable; or any Participating Entity. Vendor certifies and warrants that neither it nor its principals have been convicted of a criminal offense related to the subject matter of this solicitation.

☑ By checking this box I acknowledge that I am bound by the terms of the Proposer's Affidavit, have the legal authority to submit this Proposal on behalf of the Proposer, and that this electronic acknowledgment has the same legal effect, validity, and enforceability as if I had hand signed the Proposal. This signature will not be denied such legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation. - Jamaal Smith, Vice President of Sales and Business Development Private Networks, Kajeet, Inc.

The Proposer declares that there is an actual or potential Conflict of Interest relating to the preparation of its submission, and/or the Proposer foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the bid.

○ **Yes** ◉ **No**

The Bidder acknowledges and agrees that the addendum/addenda below form part of the Bid Document.

Check the box in the column "**I have reviewed this addendum**" below to acknowledge each of the addenda.

File Name	I have reviewed the below addendum and attachments (if applicable)	Pages
Addendum_7_Private_Wireless_Services_RFP_020624 Fri February 2 2024 10:45 AM	☑	1
Addendum_6_Private_Wireless_Services_RFP_020624 Wed January 31 2024 08:09 AM	☑	1
Addendum_5_Private_Wireless_Services_RFP_020624 Tue January 30 2024 12:22 PM	☑	3
Addendum_4_Private_Wireless_Services_RFP_020624 Fri January 26 2024 03:28 PM	☑	2
Addendum_3_Private_Wireless_Services_RFP_020624 Wed January 24 2024 04:00 PM	☑	3
Addendum_2_Private_Wireless_Services_RFP_020624 Thu January 18 2024 08:22 AM	☑	2
Addendum_1_Private_Wireless_Services_RFP_020624 Fri January 12 2024 02:04 PM	☑	1