



**BROWARD COUNTY
CONVENTION
CENTER** | GREATER FORT
LAUDERDALE

Request for Proposal
Parking Access & Revenue Control System at the Broward County
Convention Center
Bid Package Number: RFP 159-09-2026

Proposal Due Date: Monday, November 16, 2026

Issue Date: Thursday, September 23, 2026

Issued By: SMG INC.
1950 Eisenhower Blvd.
Ft Lauderdale, FL 33316

TABLE OF CONTENTS

SECTION 1 - INVITATION TO BID	4
1.01 Introduction	4
1.02 Bid Due Date.....	4
1.03 Obtaining Bid Documents.....	4
1.04 Questions, Clarification, and Additional Information	4
1.05 Proposal Evaluation.....	4
SECTION 2 - BID REQUIREMENT SUMMARY	5
SECTION 3 - INSTRUCTIONS TO BIDDERS.....	6
3.01 Receipt and Opening of Bid Proposals.....	6
3.02 Definitions	6
3.03 Bidder Qualifications	6
3.04 Examination of Conditions.....	6
3.05 Discrepancies, Omissions, or Interpretations	7
3.06 Proposal Form Introduction	7
3.07 Addenda.....	8
3.08 Sales Tax.....	8
3.09 Withdrawal or Revision of Bid Proposals.....	8
3.10 Acceptance and/or Rejection of Bid Proposals.....	8
3.11 Acceptance of Bid (Award)	8
3.12 Post-Bid Interview/Presentation.....	8
3.13 Insurance Requirements.....	9
3.14 Historically Underutilized Businesses and Equal Employment Opportunity	9
3.15 Certified Business Enterprise (CBE) Vendor.....	9
3.16 Security.....	9
3.17 ADA	9

Parking Access & Revenue Control System

BCCC/SMG

3.18	Safety	9
3.19	Clean Up and Rubbish Removal	10
3.20	Material Storage	10
3.21	Permits and Fees	10
3.22	Agreement	10
3.23	Proposal Form:	11
SECTION 4 - SCOPE OF SERVICES		12
4.01	Scope of Work	12
4.02	Additional Information	15
4.03	Submittals	16
4.04	Term of Agreement	16
4.05	Service Call Procedures	16
4.06	Billing	16
4.07	LEED Certification	17
SCHEDULE 1: Request for Additional Information		18
SCHEDULE 2: Service Agreement		19
SCHEDULE 3: SMG's Contractor Safety Program		36
SCHEDULE 4: Location Certification Form		37
Evaluator Scorecard		39
Vendor Security Questionnaire		40

SECTION 1 - INVITATION TO BID

1.01 Introduction

- A. SMG is the manager of a facility commonly known as Broward County Convention Center (the "Facility") located in Fort Lauderdale, Florida, which is owned by Broward County (the "Owner"), who, in turn, hired SMG to run the day-to-day operations of the Facility. SMG is seeking to engage An independent contractor to provide a modern Parking Access and Revenue Control System at the Broward County Convention Center. This document outlines the scope of work for the project, including all necessary equipment, tools, installation labor, supervision, licenses, permits, taxes, and deliverables, as further described herein (the "Services")

1.02 Bid Due Date

- A. Bids are due on Monday, November 16, 2026, no later than 2pm EST. Bids received after the aforementioned time will be considered non-responsive and will be returned to the Bidder unopened.
- B. Bids should be enclosed in a sealed envelope and marked: Sealed Bid For:, Parking Access and Revenue Control System, RFP 159-09-2026
- C. Bids may be mailed, or hand delivered to Ms. Ruth Fay, SMG-Broward County Convention Center, 1950 Eisenhower Blvd, Ft. Lauderdale, FL, 33316.
- D. Bidders must submit three (3) bound and sealed original bids to the address above, with full proposal, which must include all required submittals as described within the Invitation to Bid.
- E. Faxed or emailed Bids will **NOT** be accepted or considered.

1.03 Obtaining Bid Documents

- A. Bid Documents may be obtained from: BIDSUSA, Unicom Systems Inc, www.bidsusa.net and on the facility website, www.ftlauderdalecc.com/rfp/
- B. Bids submitted based on partial sets of documents will NOT be considered. Bidders are responsible for reviewing, in detail, all available Bid Documents prior to submitting their Bid.

1.04 Questions, Clarifications, and Additional Information

- A. Questions, clarifications, and requests for additional information regarding the Bid Documents **MUST** be submitted in writing, via email to bcccrfp@ftlauderdalecc.com using the form provided as Schedule 1 by the date provided in Section 2 below. In the subject line you **MUST** specify bid number and name. All questions will be answered via email in an addendum and provided to all Bidders.
- B. Telephone inquiries for clarification or interpretation of the documents **WILL NOT** be accepted.

1.05 Proposal Evaluation

- SMG may require clarification or additional information with respect to a submitted proposal. When evaluating a proposal, SMG considers the "total value" of the proposal. Total value considerations may include, but not be limited to, price, quality, product design, marketability, and durability, as well as the end user's recommendation or experience with the goods/service, the vendor's present and past performance and financial stability. **Pricing is not the only consideration.** All vendors will be notified whether or not they are selected. SMG **will not** share a vendor's specific proposal with other vendors. It is the intent of SMG to recommend contract award to the Bidder that receives the highest overall evaluation criteria score and otherwise meets all requirements of this solicitation.
- A. SMG reserves the right to reject any and all bids and to waive any informality in Bids received.
 - B. Bidders shall be aware that SMG reserves the right to hold bids for up to 90 days prior to selection of the winning Bidder.

END OF SECTION 1

SECTION 2 - BID REQUIREMENT SUMMARY

Bid Package	Parking Access and Revenue Control System
Bid Package Number	RFP 159-09-2026
MANDATORY Pre-Bid Conference & OPTIONAL Campus Tour (MAX 2 people)	Yes
Pre-Bid Conference Location	Broward County Convention Center, 1950 Eisenhower Blvd, Fort Lauderdale, FL 33316
Submit Number & Names of Attendees for the Pre-Bid Conference via email to bcccrfp@ftlauderdalecc.com . Subject line MUST contain bid number and name.	Wednesday, October 7, 2026
Pre-Bid Conference Date	Monday, October 19, 2026
Pre-Bid Conference Time & Location (Room Number)	East Admin. Conference Room, 1 pm EST.
Deadline for Questions	Monday, November 2, 2026
Bid Due Date	Monday, November 16, 2026
Bid Due Time	By 2 PM EST
Post Bid Interview/Presentation Location	Broward County Convention Center, Room number TBD
Post Bid Interview/Presentation Date	N/A
Post Bid Interview/Presentation Time	N/A
Business Location	Refer to Location Certificate Form, Schedule 4 , and submit as instructed.
Taxable	Yes
Term	Three (3) years beginning with one (1) year "No Fault" trial period.
Contract Option	SMG may, at its discretion, extend the Term for two (2) additional one (1) year terms
Contract Start Date	Upon award of contract
Service Agreement Required	Yes

END OF SECTION 2

SECTION 3 - INSTRUCTIONS TO BIDDERS

3.01 Receipt and Opening of Bid Proposals

- A. SMG is requesting Bids for the Services indicated in SECTION 1 – INVITATION TO BID as specified herein.
- B. SMG will privately open Bids.
- C. Bidders are required to fill in all blank spaces for Bid Prices on the Proposal Form.
- D. Bidders may, if indicated in the Bid Requirement Summary, be required to attend a Pre-Bid Conference to review the Bid Documents and Scope of Work with SMG.

3.02 Definitions

- A. "Addenda" are written and graphic instruments that modify or interpret the Bid Documents by additions, deletions, clarifications, or corrections. SMG may issue them prior to Bid Award. Addenda will become part of the Bid Documents when issued.
- B. "Base Bid" or "Bid" is the sum stated in the Bid Documents for which the Bidder offers to perform the work described. Base Bid is a complete and properly signed Bid to provide the services specified in the Bid Documents for the sums stipulated, supported by any submittals required in the Bid Documents.
- C. "Bid Documents" means this RFP, and any yet to be issued Addenda to this RFP and the Service Agreement.
- D. "Bidder" means an entity reviewing and responding to this Bid.
- E. "Event" means a convention, exhibit, exposition, public show, trade show or other event of a similar nature occurring at the Facility.
- F. "Facility" means the multi-purpose Broward County Convention Center.
- G. "Owner" means Broward County.
- H. "Provider" means the Bidder awarded the final contract for services.
- I. "Services" means those items described in SECTION 4 – SCOPE OF SERVICES contained in this Bid package.

3.03 Bidder Qualifications

- A. SMG reserves the right to review and accept the qualifications of all Bidders.
- B. Bidder's experience must include but is not limited to, Convention Centers, Arenas, and Large Exhibition Halls. Five (5) years' experience with Parking Access & Revenue Control. **Bidders shall provide examples of comparable gateless/free-flow parking deployments, preferably in high-volume settings.**
- C. Bidder shall provide all necessary qualified personnel, tools, and equipment to perform the required services.
- D. Bidder shall ensure that all personnel will have the necessary licenses and certifications to work on the Facility's Parking Access and Revenue Control System
- E. Bidder must be able to prove sufficient financial ability to provide the services specified in the Bid Documents.

3.04 Examination of Conditions

The Bidder is responsible for examining the premises, site, and any conditions that may impact the Bidders work. Bidders must satisfy themselves as to the condition of the premises, any

BCCC/SMG

obstruction, unusual conditions, or requirements necessary for carrying out the work, before the delivery of this proposal. A tour will be conducted at the Pre-Bid Conference, scheduled as above. Bidder is required to provide all required coordination and supervision when Bidder's work connects to or is affected by the work of others working in the Facility. Bidder to be mindful that we are an event driven facility and must minimize any possible interference with events or meetings.

3.05 Discrepancies, Omissions, or Interpretations

- A. Bidder shall promptly notify SMG of any ambiguity, inconsistency, or error that they discover upon examination of the Bid Documents or of the site and local conditions.
- B. Requests for interpretations, clarifications, or additional information must be made on the Request for Additional Information Form attached to this Bid Document as Schedule 1: Request for Additional Information. Interpretations will **NOT** be made orally. Telephone inquiries for clarification or interpretation of the Bid Documents will **NOT** be accepted.
- C. Notification of request for interpretation or correction of any ambiguity, inconsistency, or error therein which it may discover to SMG shall be made no later than the date and time noted herein as the deadline for questions in Section 2.
- D. Any interpretation, correction, or change of the Bid Documents will be made in writing by Addendum and issued to the Bidders by SMG. Interpretations, corrections, or changes of the Bid Documents made in any other manner will **NOT** be binding, and Bidders shall not rely upon such interpretations, corrections, and changes.
- E. SMG will not be responsible for any oral instructions by, or any written confirmations of any oral instructions from any Bidder, Sub-Bidder, Product Supplier, etc.

3.06 Proposal Form Introduction

- A. Each Bid shall be submitted on the Proposal Form furnished with the Bid Documents. All blanks on the Proposal Form shall be filled in, whether electronically or manually. Any Bids not submitted on the form provided may be considered non-responsive, at SMG's sole discretion.
- B. The submission of a Bid shall be evidence that the Bidder has made all necessary examinations and is satisfied as to the conditions to be encountered in performing the work and as to the requirements of all Bid Documents.
- C. Bids by corporations or other entity types shall indicate the legal name of the corporation, followed by the name of the State where incorporated/formed and must be signed by the President, Secretary, or one of the other officers of the corporation. The signature of a person authorized as agent to bind any of the above will be acceptable provided the Bid is accompanied by a proper Power-of-Attorney. Bids by corporations shall have the corporate seal affixed adjacent to the signature.
- D. All signatures shall be in ink or by digital signature and the name of the persons signing shall also be typed or printed below the signature followed by a title showing the relationship to the bidding organization such as: "Owner" in the case of a sole Owner, "Partner" in the case of a Partnership; "President", "Vice President", "Secretary", or "Treasurer" in the case of a corporation; "Agent" in the case of someone acting as Agent or Attorney-in-Fact.
- E. Bids must be received at the designated location prior to the Bid Due Date and Bid Due Time as indicated in this RFP or for any extension specified in an Addendum, if any. Bids received after designated Bid Due Date and Bid Due Time may, at the sole discretion of SMG, be considered non-responsive.

3.07 Addenda

- A. Any binding interpretation will be made only by written Addenda duly issued and a copy of such Addenda will be mailed or emailed to the last known address of each Bidder who has received Bid Documents.
- B. SMG is not responsible for the delivery of Addenda or accountable for the late delivery of Addenda. Each Bidder shall ascertain prior to submitting a Bid, that all Addenda issued have been received.
- C. Copies of Addenda will be made available for inspection wherever Bid Documents are on file for that purpose.
- D. All Addenda issued during the Bid process shall become part of the Bid Documents and receipt thereof shall be acknowledged on the Bid Proposal Form.

3.08 Sales Tax

- A. This project is **NOT** exempt from sales and/or use tax.

3.09 Withdrawal or Revision of Bid Proposals

- A. Any Bid may be withdrawn or revised in writing prior to the scheduled time for opening of Bid.
- B. A Bid may not be modified, withdrawn, or canceled by the Bidder during the stipulated time period following the time and date designated for the receipt of Bids.
- C. Bids submitted early may be modified or withdrawn only by notice to the party receiving Bids at the designated place and prior to the time for receipt of Bids. Such notice shall be in writing over the signature of the Bidder.

3.10 Acceptance and/or Rejection of Bid Proposals

- A. No Bid shall be withdrawn for ninety (90) calendar days after the Bid opening.
- B. SMG reserves the right to accept or reject any or all Bids or parts of any Bid or waive any informality or irregularity which, in SMG's judgment, is in its best interest of the project.
- C. SMG reserves the right to reject any or all Bids if responses to the above, or any other information in SMG's judgment, are unsatisfactory or do not meet the budget, or required performance standards.

3.11 Acceptance of Bid (Award)

- A. It is the intent of SMG to recommend contract award to the Bidder that receives the highest overall evaluation criteria score and otherwise meets all requirements of this solicitation.
- B. SMG may make on-site inspections of facilities where participant provides services similar to the services requested hereunder before the award of Bid.

3.12 Post-Bid Interview/Presentation

- A. After the Bids are received, tabulated, and evaluated by SMG, certain Bidders may be asked to meet with SMG for a post bid interview/presentation.
- B. The post bid interview may include, but not be limited to, a review of the Bid, financial ability of Bidder to perform the scope of services requested and Bidder's approach to the work.

3.13 Insurance Requirements

Required as set forth in Schedule 2: Service Agreement.

3.14 Historically Underutilized Businesses and Equal Employment Opportunity

- A. Bidder will not discriminate against any employee or applicant for employment because of race, color, religion, sex, age, disability, or national origin; and will take affirmative action to ensure that its applicants are employed, and its employees are treated fairly during employment without regard to their race, color, religion, sex, age, disability or national origin.
- B. Such non-discrimination shall include, but not be limited, to the following areas of employment practice: employment, upgrading, demotion, or transfer; recruitment and recruitment advertising; layoff and termination; rates of pay and other forms of compensation; and selection for training, including apprenticeship. Such shall be posted in conspicuous places, available to its employees and applicants for employment, notices setting forth the policies of non-discrimination.

3.15 Certified Business Enterprise Vendors (CBE)

- A. As part of the RFP process, CBE Vendors are encouraged to submit their proposals. Vendors with CBE-Certification should include proof of same with their submission. All vendors, including CBE-certified business, will be evaluated fairly and equitably based on the quality, value and alignment of the project requirements.
- B. Information on CBE certification, information, and requirements can be found by clicking on [this link](#).

3.16 Security

Bidder shall comply with all Facility Regulations at all times while at the Facility.

3.17 ADA

Bidder shall comply with all applicable ADA laws and regulations and train staff regularly on those regulations.

3.18 Safety

- A. The Bidder shall review and comply with SMG's Contractor Safety Program, attached hereto as Schedule 3.
- B. The Bidder is responsible for submitting, paying for, maintaining, delivering, and posting all applicable professional licenses, certifications or permits required by Federal, State, and Local Law.
- C. The Bidder shall submit a copy of its safety and health program, including training, which must meet or exceed all applicable Federal, State, and Local Standards and the SMG Safety Programs.
- D. The winning Bidder shall submit a copy of any and all licenses, certifications and/or permits as required to perform these services.
- E. The winning Bidder shall comply with all applicable OSHA, Federal, State, and Local Laws, Rules, and Regulations.
- F. Safety Data Sheets must be submitted to SMG for all supplies and chemicals intended for use in the performance of the Services. All chemicals used at the Facility shall carry an EPA approval number.

3.19 Clean Up and Rubbish Removal

Waste generated by Provider must be removed by the Provider in a timely and acceptable manner to the satisfaction of SMG.

3.20 Material Storage

Provider is responsible for storing any materials and equipment used to provide the Services and such must be stored following manufacturer guidelines. SMG shall endeavor to make a reasonable amount of space, if available, to Provider for storage.

3.21 Permits and Fees

The Bidder shall secure and pay for any permits, governmental fees, licenses, and inspections, required to provide the Services.

3.22 Service Agreement

Attached as Schedule 2 is the SMG Service Agreement ("Service Agreement") which the winning Bidder will be required to enter with SMG. If the winning Bidder refuses to enter into the Service Agreement (or insists on changing/modifying the Service Agreement) with SMG, SMG reserves the right to award the Bid to another Bidder. SMG reserves the right to make non-substantive changes to the Service Agreement prior to execution, which shall not invalidate this section.

PLEASE SUBMIT A DETAILED PRICING SHEET.

Provide clear pricing structure, including but not limited to:

- Upfront Costs
 - Hardware
 - Signage
 - Installation, Configuration, Implementation
- Ongoing Costs / Fees
 - Software licensing
 - Support and maintenance
 - Payment processing fees
 - Collection-related fee
- Revenue Sharing/Commission Structure:

Bidders shall clearly identify any proposed revenue-sharing models, commission structures, transaction-based fees, convenience fees, enforcement revenue participation, or other recurring financial arrangements associated with the proposed solution. Bidders shall provide sufficient detail to allow the County to fully evaluate the long-term financial impact of the proposed system.

END OF SECTION 3

SECTION 4- SCOPE OF SERVICES

4.01 Scope of Work

Broward County is seeking proposals from qualified providers for the deployment of a modern Parking Access and Revenue Control System (PARCS) at the Broward County Convention Center ("BCCC"). The County intends to implement a gateless / free-flow parking system, supported by license plate recognition (LPR) and a fully integrated technology platform. This RFP is for equipment, technology, and support services only. The County will operate the parking system internally. The County seeks a turnkey system that replaces traditional gated parking systems, supports modern payment methods, provides real-time reporting, and enhances the customer parking experience. Bidders shall provide examples of comparable gateless/free-flow parking deployments, preferably at convention centers, airports, municipalities, entertainment venues, or other high-volume facilities.

Objectives

- Replace traditional gated PARCS functionality with a modern gateless system.
- Utilize LPR as the primary payment verification and compliance mechanism.
- Provide multiple payment options (mobile, reservations, subscriptions, pay machines, etc.)
- Deliver real-time occupancy and revenue reporting.
- Enable validation, discounting, and promotional tools.
- Provide 24/7/365 customer support.
- Include local technical support and troubleshooting.
- Provide ongoing operational consulting.

System Architecture

Provider shall identify guaranteed system uptime percentage and associated service level agreements (SLAs).

The proposed solution shall be:

- Cloud-based or hybrid.
- Fully integrated across all modules.
- Managed through a single administrative platform.
- Designed to minimize reliance on multiple providers or disconnected systems.

Connectivity: Provider shall clearly identify

- Minimum bandwidth requirements.
- Network architecture requirements.
- Cellular and/or internet dependencies.
- Redundancy recommendations.
- Cybersecurity requirements and protocols.
- Outline offline operational capabilities and LPR functionality during outages.

Data Ownership and Security

All system data generated through operation of the PARCS solution shall remain the sole property of Broward County. Provider shall comply with all applicable cybersecurity, Payment Card Industry Data Security Services (PCI-DSS), and data privacy standards applicable to the proposed solution. Provider shall not sell, disclose, distribute, or otherwise use County data for any purpose other than performing the services described in this Agreement without the prior written consent of the County.

The Provider shall identify and describe, at a minimum, the following:

- Data storage location(s).
- Hosting environment(s).
- Data retention policies.
- Backup and disaster recovery procedures.
- Cybersecurity protections and standards.

Payment Capabilities

The system shall support:

- Mobile / Web Payments (QR-Code enabled.).
- Pay-on-foot / Pay Machine Payments.
- Reservations.
- Subscriptions.
- Validations, Discounting, and Promotional Tools.

Payment Processing and Compliance

Provider shall:

- Comply with all current Payment Card Industry Data Security Standards (PCI-DSS).
- Ensure the secure processing, transmission, and storage of all payment card information.
- Maintain appropriate safeguards to protect payment transactions and customer financial data.
- Provide documentation demonstrating PCI-DSS compliance upon request.

Audit and Compliance Rights

Provider shall:

- Maintain records sufficient to demonstrate compliance with the requirements of the Agreement.
- Cooperate with reasonable audits conducted by Legends Global or its authorized representatives.
- Provide supporting documentation related to system security, payment processing, operational performance, and compliance upon request.
- Promptly address and remediate any deficiencies identified during an audit.

Real-Time Occupancy & Reporting

The system shall provide:

- Real-time occupancy tracking, space counting, and directional signage.
- Zone-based counts.
- Customer-facing digital occupancy signage.
- Dashboard analytics.
- Exportable data.
- API (Application Programming Interface) integration capability for future signage expansion.

Compliance & Enforcement

Provider must demonstrate a proven ability to achieve high compliance in a gateless environment and provide documented compliance metrics from comparable gateless deployments.

Submissions must include:

- Compliance strategy and methodology.
- Notice and escalation processes.
- Integration with collections services.

Customer Support

Provider shall maintain 24/7/365 customer support, including:

- Live call center support.
- Payment and transaction assistance.
- Issue resolution and escalation.

Local Technical Support

Provider shall supply local technical support, including:

- Troubleshooting and issue resolution.
- System monitoring.
- Maintenance coordination.

Incident Response and Breach Notification

Provider shall supply:

- Prompt investigation of any actual or suspected cybersecurity incident.
- Notification to Legends Global, without unreasonable delay, of any confirmed or suspected data breach affecting the proposed system.
- Full cooperation with Legends Global in incident response, remediation, and recovery efforts.
- A written incident response plan outlining notification procedures, escalation protocols, and corrective actions.

Operational Consulting

While the County will operate the system, the provider shall act as a technology and operations advisor, including guidance on:

- Traffic flow design in a gateless environment.
- Facility configuration.
- Recommendations for system optimization.

Monthly Performance Reviews

Provider shall deliver monthly performance reviews with BCCC staff, including:

- System performance metrics.
- Compliance rates.
- Revenue trends.
- Operational insights.
- Recommendations for improvement.

Implementation & Training

The County intends to require a one (1) year no-fault trial period. During this period the County reserves the right to terminate the agreement without cause, should the proposed solution fail to meet operational expectations, compliance targets, customer experience objectives, or system performance standards.

Provider shall outline:

- How a no-fault period would be structured.
- Transition planning and operational safeguards.
- Removal or transfer of installed equipment.
- Restoration or protection of County infrastructure (booths, electrical infrastructure, network infrastructure, signage, parking assets etc.)
- Risk mitigation measures during implementation and potential decommissioning.
- Any associated costs or financial considerations.

Provider shall furnish:

- Full implementation plan.
- System configuration.
- Testing and validation.
- Staff training.
- Go-live support.
- Ongoing optimization.

4.02 Additional Information

1. Provider is required to obtain and pay for any fees and licenses as required by Federal, State and Local governing bodies and codes.
2. Provider shall provide all hoisting, conveying equipment, and swing stages as required to unload, stock, distribute, handle, and install the work of this scope.
3. Provider is required to provide all required coordination and supervision where Provider's work connects to or is affected by the work of others working in the Facility.
4. Provider shall coordinate installation of the Scope of Work with the work of other trades to ensure conformance with the requirements of the Contract Documents. Conflicts arising from this Provider's failure to coordinate will be the responsibility of the Provider to resolve.

4.03 Submittals

SMG requires Bidders to submit the following documentation in the following order. Failure to do so may result in the response being rejected.

1. Detailed Quotation.
2. Summary Bid.
3. Technical Proposal / System Description.
4. Implementation and Transition Plan.
5. Service, Support and Maintenance Plan.
6. Data Security and Compliance Documentation.
7. No-Fault Trial Period Plan
 - a. Provide a proposed approach for the one-year No-Fault Trial Period, including performance monitoring, success measures, transition safeguards, termination

procedures, removal or transfer of equipment, restoration of County infrastructure, and any costs associated with termination or transition.

8. Client References.
9. Sample Certificate of Insurance acknowledging coverages required.
10. Location Certification Form.
11. Bidder Disclosures (if any).
12. Bidder Financial Information, including, but not limited to, audited financial statements of the Bidder, if available, for its two (2) most recent fiscal years, including balance sheets and profit and loss statements, prepared, and certified by an independent certified public accountant.
13. Vendor Security Questionnaire on page 40 of the document must be filled out and returned as part of your bid.

4.04 Term of Agreement

The initial term of the proposed agreement for the Services is anticipated to be three (3) years, including an initial one (1) year "No Fault" trial period. SMG may, at its discretion, extend the Agreement for two (2) additional one (1) year renewal terms.

4.05 Service Call Procedures

Provider MUST schedule service calls and check-in with BCCC Parking Manager prior to performing any work.

4.06 Billing

SMG requires detailed monthly invoices for all services including, but not limited to, the following:

1. Labor and service charges
2. Hardware and equipment costs
3. Software licensing fees
4. Maintenance and support fees
5. Transaction and payment processing fees
6. Citation and collections-related fees
7. Emergency callout charges, if applicable

Monthly invoices shall include supporting operational and revenue reports, including transaction activity and applicable revenue-sharing calculations.

Failure to provide complete and accurate invoices may result in delayed payments.

What is LEED Certification?

Leadership in Energy and Environmental Design (LEED) is a voluntary green building certification program developed by the U.S. Green Building Council (USGBC) and launched in 1998. Demand for LEED certification has grown significantly among building owners, developers, and property managers. Many city, state, and federal agencies either require LEED certification for public facilities or offer incentives such as tax credits and grants to encourage adoption among private developers.

LEED certification evaluates projects based on criteria including sustainable site development, energy and water efficiency, use of sustainable and recyclable materials, and indoor environmental quality. The program applies to a wide range of project types, including new construction, existing buildings, healthcare, retail, and schools.

LEED uses a point-based rating system with a maximum of 100 base points. Projects achieving 40 points or more may be certified, with higher levels of certification awarded at Silver, Gold, and Platinum thresholds.

For more information, visit www.usgbc.org

- The work of this Agreement shall comply with all LEED – Gold requirements where applicable. This shall include providing requirements for regional materials, products with recycled content and low VOC components, and participation in the construction waste diversion plan.
- This Bidder shall, on a daily basis, perform clean-up and trash removal of all debris generated by this Bidder to a central site container as directed by SMG. Debris generated by this Bidder shall be sorted and placed into appropriate dumpsters provided by SMG to assist in recycling efforts and LEED compliance. Haul-off will be by others. Disposal and removal from the site of excess finish materials, residue from cleanup of installation materials, and other hazardous waste shall be done in accordance with governmental regulations and shall be the responsibility of this Bidder.

END OF SECTION 4

SCHEDULE 1: Request for Additional Information

To	Ms. Ruth Fay		
Address	1950 Eisenhower Blvd., Ft. Lauderdale, FL 33316		
Phone Number	954.302.8866	Email address:	bcccrfp@ftlauderdalecc.com
Bid Package	Parking Access and Revenue Control System		
Bid Package Number	RFP 159-09-2026		
Date of Request			
<i>Bidder Information</i>			
Name			
Company			
Address			
Phone Number			
E-Mail Address			
<i>Request For Clarification, Interpretation or Additional Information</i>			

SCHEDULE 2
SERVICE AGREEMENT FOR
GREATER FORT LAUDERDALE/BROWARD COUNTY CONVENTION CENTER

This service agreement (together with the Exhibits attached hereto, the ("Agreement")) is made and entered into by and between SMG, a Pennsylvania General Partnership, with an address at 1950 Eisenhower Blvd. Fort Lauderdale, FL 33316 ("SMG") and _____ (the "Provider" a Florida Corporation) whose current address is _____
(each a "Party" and collectively referred to as the "Parties").

BACKGROUND

SMG is the manager of the Greater Fort Lauderdale/Broward County Convention Center (the "**Facility**"), located in Fort Lauderdale, Florida, which is owned by Broward County, a political subdivision of the State of Florida (the "**Owner**"). Pursuant to an agreement between SMG and Owner, SMG manages and operates the Facility (the "Management Agreement"). SMG desires to obtain the services of an independent company to perform certain functions relating to the Facility, as more particularly described in this Agreement. Provider must have the personnel, material, equipment, and skills to perform the types of services desired by SMG, as more particularly described in this Agreement. Accordingly, SMG desires to obtain those services from Provider, and Provider desires to perform those services for SMG, in accordance with the terms and conditions set forth herein.

NOW, THEREFORE, for good and valuable consideration, including the foregoing, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Description of Services. Provider shall perform all Services (as defined below), including, without limitation, the work specified in Exhibit A (the "**Scope of Services**"), and in doing so must comply with the terms of the Management Agreement. The Scope of Services is a description of Provider's obligations and responsibilities and is deemed to include preliminary considerations and prerequisites, And all labor, materials, equipment, and tasks that are such an inseparable part of the work and services described that exclusion would render performance by Provider impractical, illogical, or unconscionable.

For purposes of this Agreement, "Services" shall mean all work required of Provider under this Agreement, including, without limitation, all deliverables, goods, consulting, training, project management, and services specified in the Scope of Services attached as Exhibit A.

2. Payment for Services. For all Services provided under this Agreement, SMG will pay Provider up to a maximum amount as follows:

Services/Goods	Not-To-Exceed Amount
	\$
	\$
	\$
TOTAL NOT TO EXCEED	\$

Payment shall be made only for Services actually performed and completed pursuant to this Agreement, as set forth on Exhibit B (Payment Schedule), which amount shall be accepted by Provider as full compensation for all such Services.

SMG may withhold payment, in whole or in part, to the extent necessary to protect itself from loss on account of the Owner's withholding funds to SMG due to inadequate or defective work that has not been remedied or resolved to the Owner's satisfaction.

3. Term. This Agreement begins on the date it is fully executed by the Parties ("Effective Date") and continues through [_____] ("Initial Term"), unless otherwise terminated or extended as provided in this Agreement. The Initial Term and any Extension Term(s), as those terms are defined in this section, are collectively referred to as the "Term."

SMG may, in its sole discretion, extend this Agreement for up to two (2) additional one (1) year terms (each an "Extension Term") by sending written notice of extension to Provider at least ninety (90) days prior to the expiration of the then-current term. Unless expressly stated in Exhibit B, Provider shall be compensated at the rates in effect when an Extension Term was invoked by SMG and shall continue to provide the Services upon the same terms and conditions as set forth in this Agreement for such extended period.

4. Default and Termination.

- (a) Default. Provider shall be in default under this Agreement if any of the following occur: (I) Provider or any of its officers, employees, or agents fail to perform or fulfill any term, covenant, or condition contained in this Agreement and Provider fails to cure such default within five (5) calendar days after Provider has been notified in writing of such default; (ii) Provider makes a general assignment for the benefit of creditors; (iii) the filing by or against Provider of any petitions in bankruptcy either voluntary or involuntary, (iv) any transfer, assignment, or the passing of any benefits, rights, or obligations of this Agreement to creditors, assignees, or transferees of Provider without the prior written approval of SMG, which may be withheld in its sole and absolute discretion; (v) the abandonment or discontinuance by Provider, without written consent of SMG, of any or all of the Services permitted or required herein; or (vi) if Provider was a certified CBE or SBE with Broward County on the Effective Date of this Agreement, a failure to maintain such certification through the Term.

SMG shall be in default under this Agreement if SMG fails to perform or fulfill any term, covenant, or condition contained in this Agreement and SMG fails to cure such default within thirty (30) business days after SMG has been served with written notice of such default or SMG makes a general assignment for the benefit of creditors. SMG shall not be deemed to be in default under this Agreement if SMG fails to pay any of the fees due hereunder as a result of Provider's default under this Agreement.

Nothing herein shall be construed as excusing either Party from diligently commencing and completing a cure within a lesser time if reasonably possible.

- (b) Termination. Upon a default pursuant to Section 4(a) hereof, the non-breaching Party may, at its option, upon written notice or demand upon the other Party, terminate this Agreement.
5. Insurance. Throughout the Term, Provider shall, at its sole expense, maintain the minimum insurance coverages stated in Exhibit C (Insurance) in accordance with the terms and

conditions of this section and Exhibit C. Provider shall ensure that SMG and Owner are listed and endorsed as additional insureds on all policies required under this section and Exhibit C. At least thirty (30) days prior to commencement of this Agreement, Provider shall provide SMG with a copy of all Certificates of Insurance or other documentation sufficient to demonstrate the insurance coverage required in this section and Exhibit C. Provider shall maintain insurance coverage against claims relating to any act or omission by Provider, its agents, representatives, employees, or subcontractors in connection with this Agreement. SMG reserves the right at any time to review and adjust the limits and types of coverage required under this article and Exhibit C.

6. INDEMNIFICATION.

PROVIDER SHALL INDEMNIFY, HOLD HARMLESS, AND DEFEND SMG AND OWNER, AND ALL OF THEIR CURRENT, PAST, AND FUTURE OFFICERS, AGENTS, AND EMPLOYEES (COLLECTIVELY, "INDEMNIFIED PARTY") FROM AND AGAINST ANY AND ALL CAUSES OF ACTION, DEMANDS, CLAIMS, LOSSES, LIABILITIES, AND EXPENDITURES OF ANY KIND, INCLUDING ATTORNEYS' FEES, COURT COSTS, AND EXPENSES, INCLUDING THROUGH THE CONCLUSION OF ANY APPELLATE PROCEEDINGS, RAISED OR ASSERTED BY ANY PERSON OR ENTITY NOT A PARTY TO THIS AGREEMENT, AND CAUSED OR ALLEGED TO BE CAUSED, IN WHOLE OR IN PART, BY ANY BREACH OF THIS AGREEMENT BY PROVIDER, OR ANY INTENTIONAL, RECKLESS, OR NEGLIGENT ACT OR OMISSION OF PROVIDER, ITS OFFICERS, EMPLOYEES, OR AGENTS, ARISING FROM, RELATING TO, OR IN CONNECTION WITH THIS AGREEMENT (COLLECTIVELY, A "CLAIM"). IF ANY CLAIM IS BROUGHT AGAINST AN INDEMNIFIED PARTY, PROVIDER SHALL, UPON WRITTEN NOTICE FROM SMG, DEFEND EACH INDEMNIFIED PARTY WITH COUNSEL SATISFACTORY TO SMG AND OWNER, OR, AT SMG'S OPTION, PAY FOR AN ATTORNEY SELECTED BY SMG AND OWNER TO DEFEND THE INDEMNIFIED PARTY. THE OBLIGATIONS OF THIS SECTION SHALL SURVIVE THE EXPIRATION OR EARLIER TERMINATION OF THIS AGREEMENT. IF CONSIDERED NECESSARY BY SMG, ANY SUMS DUE PROVIDER UNDER THIS AGREEMENT MAY BE RETAINED BY SMG UNTIL ALL CLAIMS SUBJECT TO THIS INDEMNIFICATION OBLIGATION HAVE BEEN SETTLED OR OTHERWISE RESOLVED.

THE OBLIGATIONS OF THIS SECTION SHALL SURVIVE THE EXPIRATION OR EARLIER TERMINATION OF THIS AGREEMENT.

7. Compliance with Laws. Provider and the Services must comply with all applicable laws, codes, advisory circulars, rules, regulations, or ordinances of any federal, state, county, municipal, or other governmental entity, as may be amended.
8. Review and Audit Privileges. Provider and all of its subcontractors shall preserve and make available, at reasonable times within Broward County, Florida, for examination and audit, full and accurate books, records, and accounts of Provider and its subcontractors that are related to this Agreement (collectively, the "**Records**"), during the Term and for at least three (3) years following the expiration or termination of this Agreement or until resolution of any audit findings, whichever is longer. This section shall survive any dispute or litigation between the Parties, and Provider expressly acknowledges and agrees to be bound by this section throughout the course of any dispute or litigation with SMG and/or Owner. Any audit or inspection pursuant to this section may be performed by SMG or any of its designated representatives (which representatives may include, without limitation, independent auditors). Provider hereby grants SMG the right to conduct such audit or review at Provider's place of business, if deemed appropriate by SMG, with seventy-two (72) hours' advance notice. Provider shall make all such records and documents available electronically in common file formats or via remote access if, and to the extent, requested by SMG. Provider and its subcontractors shall also provide, at Provider's own expense, copies of all

or a portion of the Records when so requested by SMG.

If an audit or inspection reveals overpricing or overcharges to SMG of any nature by Provider in excess of five percent (5%) of the total billings reviewed by SMG, in addition to making adjustments for the overcharges, Provider shall pay the actual cost of such audit or, if the actual cost is unreasonably high, the reasonable cost. Any adjustments or payments due as a result of such audit or inspection shall be made within thirty (30) days after presentation of SMG's findings to Provider.

Provider shall ensure that the requirements of this section are included in all agreements with its subcontractor(s).

9. Representations and Warranties. Provider hereby represents and warrants as follows:

- (a) Provider has the full power and authority to enter into this Agreement and perform each of its obligations hereunder.
- (b) Provider represents and warrants that it possesses the knowledge, skill, experience, and financial capability required to perform and provide all Services and that Provider and each person and entity that will provide Services is duly qualified to perform such Services by all appropriate governmental authorities, where required, and is sufficiently experienced and skilled in the area(s) for which such person or entity will render such Services. Provider represents and warrants that the Services shall be performed in a skillful and respectful manner, and that the quality of all Services shall equal or exceed prevailing industry standards for the provision of such Services.
- (c) Provider represents and warrants that there is no action or proceeding, at law or in equity, before any court, mediator, arbitrator, governmental or other board or official, pending or, to the knowledge of Provider, threatened against or affecting Provider, the outcome of which may (a) affect the validity or enforceability of this Agreement, (b) materially and adversely affect the authority or ability of Provider to perform its obligations under this Agreement, or (c) have a material and adverse effect on the consolidated financial condition or results of operations of Provider or on the ability of Provider to conduct its business as presently conducted or as proposed or contemplated to be conducted.
- (d) Provider represents and warrants that all statements and representations made in Provider's proposal, bid, or other supporting documents submitted to SMG in connection with the solicitation, negotiation, or award of this Agreement, including during the procurement or evaluation process, were true and correct when made and are true and correct as of the date Provider executes this Agreement, unless otherwise expressly disclosed in writing by Provider.
- (e) Provider represents and warrants that it has not employed or retained any person or entity, other than a bona fide employee working solely for Provider, to solicit or secure this Agreement, and that it has not paid or agreed to pay any person or entity, other than a bona fide employee working solely for Provider, any fee, commission, percentage, gift, or other consideration contingent upon or resulting from the award or making of this Agreement.
- (f) Provider represents that it is familiar with the requirements and prohibitions under the Public Entity Crime Act, Section 287.133, Florida Statutes, and represents that its entry into this Agreement will not violate that statute. Provider further represents that there has been no determination that it committed a "public entity crime" as defined

by Section 287.133, Florida Statutes, and that it has not been formally charged with committing an act defined as a "public entity crime" regardless of the amount of money involved or whether Provider has been placed on the convicted vendor list.

- (g) Provider represents that it has not been placed on the "discriminatory vendor list" as provided in Section 287.134, Florida Statutes, and that it has not been identified as a company or other entity subject to scrutiny under Sections 215.473 or 215.4725, Florida Statutes. Provider represents and certifies that it is not, and throughout the Term will not be, ineligible to contract with SMG on any of the grounds stated in Section 287.135, Florida Statutes. Provider represents that it is, and for the duration of the Term will remain, in compliance with Section 286.101, Florida Statutes.
- (h) Prohibited Telecommunications Equipment. Provider represents and certifies that it and its subcontractors do not use, and throughout the Term will not provide or use, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, as such terms are used in 48 CFR §§ 52.204-24 through 52.204-26.
- (i) Provider acknowledges that SMG is materially relying on the representations, warranties, and certifications of Provider stated in this section, and SMG shall be entitled to exercise any or all of the following remedies if any such representation, warranty, or certification is untrue: (a) recovery of damages incurred; (b) termination of this Agreement without any further liability to Provider; (c) set off from any amounts due Provider the full amount of any damage incurred; and (d) debarment of Provider.

10. Covenants. Provider hereby covenants as follows:

- (a) Provider shall not occupy or use the Facility, nor shall interfere with the activities of the Facility, except as is reasonably necessary to perform the Services hereunder.
- (b) Provider shall not cause or permit any Hazardous Material to be used, stored, or generated on, or transported to and from the Facility. "**Hazardous Material**" shall mean, without limitation, those substances included within the definitions of "hazardous substances", "hazardous materials", "toxic substances", or "solid waste" in any applicable state or federal environmental law.
- (c) Provider shall not make any alterations or improvements to the Facility without the prior written consent of SMG.
- (d) Provider shall not operate any equipment or materials belonging to SMG without the prior written approval of SMG.
- (e) No portion of any passageway or exit at the Facility shall be blocked or obstructed in any manner whatsoever, and no exit door or any exit shall be locked, blocked, or bolted while the Facility is in use. Moreover, all designated exits shall be maintained in such manner as to be visible at all times.
- (f) Provider's employees will adhere to the provisions of the SMG Business Conduct Policy Book, SMG Human Resource Policies & Procedures, and SMG Customer Service Training, the terms of which are incorporated herein by reference.

11. Confidentiality.

SMG acknowledges that the vast majority of documents and other records related to its

operation of the Facility and to subcontractor agreements are subject to disclosure under Florida's public records laws. This section is intended to cover the limited circumstances in which SMG shares with Provider confidential or trade secret information that is separate from SMG's contract with the Owner or otherwise exempt from disclosure under Florida law. In such a case, the information could lose trade secret protection/status if SMG fails to take proper protective measures, including having confidentiality provisions like this one.

Generally, the documents, materials, and information associated with this Agreement and SMG's management and operation of the Facility are public records under Florida's public records laws and are subject to disclosure. However, in connection with the performance of the Services under this Agreement, SMG may provide to Provider confidential and/or proprietary information of SMG and its operations at the Facility that SMG believes constitutes or contains trade secrets or is otherwise exempt from production under Florida public records laws (including Florida Statutes Chapter 119) which information SMG shall separately submit and conspicuously label as "EXEMPT FROM PUBLIC RECORD PRODUCTION," "EXEMPT FROM PUBLIC RECORD PRODUCTION – TRADE SECRET," and/or "RESTRICTED MATERIAL – DO NOT PRODUCE," as applicable. As a condition to the provision of such information by SMG to Provider, Provider agrees to be bound by the terms of this Section 11. "Information" for the purpose of this section 11 shall mean information SMG has separately submitted and conspicuously labeled in accordance with this paragraph as being exempt from public record production or trade secret information.

If SMG or Provider receives a request for public records regarding this Agreement or the Services, Provider must immediately notify SMG in writing and provide all requested records to SMG to enable SMG to coordinate with the Owner to timely respond to the public records request. SMG or the Owner, as applicable, will respond to all such public records requests.

When submitting requested records to SMG in connection with a request for public records regarding this Agreement, Provider must separately submit and conspicuously label as "RESTRICTED MATERIAL – DO NOT PRODUCE" any material (a) that Provider contends constitutes or contains its trade secrets under Chapter 688, Florida Statutes, or (b) for which Provider asserts a right to withhold from public disclosure as confidential or otherwise exempt from production under Florida public records laws (including Chapter 119, Florida Statutes) (collectively, "Restricted Material"). In addition, Provider must, simultaneous with the submission of any Restricted Material, provide a sworn declaration or affidavit in a form acceptable to SMG from a person with personal knowledge attesting that the Restricted Material constitutes trade secrets or is otherwise exempt or confidential under Florida public records laws, including citing the applicable Florida statute and specifying the factual basis for each such claim. Upon request by SMG or Owner, Provider must promptly identify the specific applicable statutory section that protects any particular document. If a third party submits a request to SMG or the Owner for records designated by Provider as Restricted Material, SMG or Owner shall refrain from disclosing such material unless otherwise ordered by a court of competent jurisdiction, authorized in writing by Provider, or the claimed exemption is waived. Any failure by Provider to strictly comply with the requirements of this section shall constitute Provider's waiver of SMG's and Owner's obligation to treat the records as Restricted Material. Provider must indemnify and defend SMG, Owner, and their respective employees and agents from any and all claims, causes of action, losses, fines, penalties, damages, judgments, and liabilities of any kind, including attorneys' fees, litigation expenses, and court costs, relating to nondisclosure of Restricted Material in response to a third-party request.

IF PROVIDER HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119,

FLORIDA STATUTES, TO PROVIDER'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT 954-302-8866 bcccrfp@ftlaudalecc.com. 1950 Eisenhower Blvd, Fort Lauderdale, Florida 33316

All Information disclosed by SMG to Provider shall remain the property of SMG and shall be kept secret and confidential and be maintained in confidence by Provider and its directors, officers, employees, consultants, subcontractors, and agents. In addition, Provider and its directors, officers, employees, consultants, subcontractors, and agents shall not, without the prior written permission of SMG, disclose in any manner whatsoever, in whole or in part, or use the Information of SMG, other than for the purpose of performing its Services under this Agreement. Without limiting the foregoing, Provider shall restrict the custody, possession, knowledge, development, compilation, preparation, and use of the Information to its officers, employees, and permitted consultants, subcontractors, and agents who are directly involved in performing the Services hereunder to the extent such Information is needed in order to perform such services and then only on a confidential basis acceptable to SMG. If requested by SMG, Provider shall cause each of its officers, employees, and permitted consultants, subcontractors, and agents assigned to or otherwise involved in performing such services to agree to be bound by this Agreement as a condition of the continued provision of the Services hereunder. So long as Provider is restricted pursuant to this Section 11, Provider shall, notwithstanding the provisions of this paragraph, take all steps it would normally take to protect its own confidential information to ensure that the Information received by it shall be maintained in confidence and not disclosed or used as provided herein. Notwithstanding the foregoing, Provider shall be liable to SMG for any breaches or violations of this Agreement by any director, officer, employee, consultants, subcontractors, or agent of Provider.

Upon SMG's written request, Provider shall promptly return to SMG all Information and tangible material (including all copies, models, and samples thereof) that discloses or relates to any of the Information.

The obligations of Provider under this section 11 shall not apply to: (I) Information which, at the time of disclosure thereof, is in the public domain; (ii) Information which, after disclosure, becomes a part of the public domain by publication or otherwise, except by breach of this Agreement by Provider; (iii) Information which Provider receives from a third party who has the right to, and legally does, disclose the same to Provider; or (iv) Information which is required to be disclosed by judicial or administrative process or, in the opinion of counsel, by other mandatory requirements of law. Notwithstanding the foregoing, Information shall not be deemed in the public domain simply because it is included in more general information in the possession of Provider.

In connection with the performance of the Services hereunder, any communications, oral or written, that Provider may need to have with any other party (including without limitation the Owner or its directors, officers, employees, agents, or representatives) shall be made through SMG and its designated officers and employees, unless Provider receives the prior written consent from SMG's General Manager at the Facility.

Provider agrees that the provisions of this Agreement are reasonable and necessary to protect the interests of SMG and that SMG's remedies of law for a breach of any of the provisions of this Agreement will be inadequate and that, in connection with any such breach, SMG will be entitled, in addition to any other available remedies (whether at law or in equity), to temporary and permanent injunctive relief without the necessity of proving actual damage or immediate or irreparable harm, or of the posting of a bond. Notwithstanding the foregoing, if a court of competent jurisdiction shall determine any of

the provisions of this Agreement to be unreasonable, Provider agrees to a reaffirmation of such provisions by such court to any limits which such court finds to be reasonable and that Provider will not assert that such provisions should be eliminated in their entirety by such court. The obligations of confidentiality and non-use contained in this Section 11 shall expire five (5) years after the expiration or termination of this Agreement.

12. Construction of this Agreement.

- (a) Choice of Law. This Agreement shall be interpreted and construed in accordance with and governed by the laws of the State of Florida. The exclusive venue for any lawsuit arising from, related to, or in connection with this Agreement shall be in the state courts of the Seventeenth Judicial Circuit in and for Broward County, Florida. If any claim arising from, related to, or in connection with this Agreement must be litigated in federal court, the exclusive venue for any such lawsuit shall be in the United States District Court or United States Bankruptcy Court for the Southern District of Florida.
- (b) Interpretation. The titles and headings contained in this Agreement are for reference purposes only and shall not in any way affect the meaning or interpretation of this Agreement. All personal pronouns used in this Agreement shall include any other gender, and the singular shall include the plural, and vice versa, unless the context otherwise requires. Terms such as "herein" refer to this Agreement as a whole and not to any particular sentence, paragraph, or section where they appear, unless the context otherwise requires. Whenever reference is made to a section, paragraph, or article of this Agreement, such reference is to the section, paragraph, or article as a whole, including all subsections and subparagraphs of such section, paragraph, or article. Any reference to "days" means calendar days, unless otherwise expressly stated. Any reference to approval by SMG shall require approval in writing, unless otherwise expressly stated.
- (c) Entire Agreement; Amendments. This Agreement represents the final and complete understanding of the Parties regarding the subject matter of this Agreement and supersedes all prior and contemporaneous negotiations and discussions regarding same. All commitments, agreements, and understandings of the Parties concerning the subject matter of this Agreement are contained herein. Unless expressly authorized herein, no modification, amendment, or alteration of any portion of this Agreement is effective unless contained in a written document executed with the same or similar formality as this Agreement and by duly authorized representatives of SMG and Provider.
- (d) Severability. If any part of this Agreement is found to be unenforceable by any court of competent jurisdiction, that part shall be deemed severed from this Agreement and the balance of this Agreement shall remain in full force and effect.
- (e) Successors. This Agreement shall be binding upon, and shall inure to, the benefit of the successors and assigns of SMG, and to such successors and assigns of Provider as are permitted to succeed to the Provider's right upon and subject to the terms hereof.
- (f) Independent Contractor; No Partnership. SMG and Provider shall each be and remain an independent contractor with respect to all rights and obligations arising under this Agreement. Nothing in this Agreement shall constitute a partnership, joint venture, or any other relationship between the Parties.
- (g) Third-Party Beneficiaries. Except for Owner, who is expressly agreed to be an intended

third-party beneficiary of this Agreement, having all rights and privileges associated therewith, neither Provider nor SMG intends to primarily or directly benefit a third party by this Agreement. Therefore, the Parties acknowledge that there are no third-party beneficiaries to this Agreement and that no third party shall be entitled to assert a right or claim against either of them based upon this Agreement.

- (h) If the Management Agreement between SMG and Owner is terminated or expires for any reason, this Agreement shall remain in full force and effect. Upon such termination or expiration, Owner, or any successor operator of the Facility designated in writing by Owner, shall automatically be substituted for SMG as a party to this Agreement, without the need for further action or assignment by SMG. Owner (or its designated successor operator) shall provide written notice to Provider identifying the effective date of such substitution and the name and contact information of the successor operator, if applicable. Upon receipt of such notice, Provider shall continue performance under this Agreement without interruption, recognizing the Owner (or its designated successor operator) as the contracting party entitled to all rights, benefits, and obligations of Operator under this Agreement.

13. Miscellaneous.

- (a) Materiality and Waiver. Each requirement, duty, and obligation set forth in this Agreement was bargained for at arm's-length and is agreed to by the Parties. Each requirement, duty, and obligation set forth in this Agreement is substantial and important to the formation of this Agreement, and each is, therefore, a material term. The failure of any Party to enforce any of the provisions of this Agreement shall not be deemed a waiver of such provision or modification of this Agreement. A waiver of any breach shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of this Agreement. To be effective, any waiver must be in writing signed by an authorized signatory of the Party granting the waiver.
- (b) Assignment. All subcontractors must be expressly identified in this Agreement or otherwise approved in advance and in writing by SMG. Except for approved subcontracting, neither this Agreement nor any of the rights or obligations hereunder may be assigned, transferred, subcontracted, or encumbered by Provider without the prior written consent of SMG, as to any subcontract, and Owner, as to any assignment, transfer, or encumbrance. Any assignment, transfer, subcontract, or encumbrance in violation of this paragraph shall be void and ineffective, constitute a breach of this Agreement, and permit SMG to immediately terminate this Agreement, in addition to any other remedies available to SMG at law or in equity. Owner and SMG reserve the right to condition their approval of any assignment, transfer, subcontract, or encumbrance upon further due diligence and an additional fee paid to SMG or Owner to reasonably compensate it for the performance of any such due diligence.
- (c) Notices. Any notice, consent, or other communication given pursuant to this Agreement shall be in writing and shall be effective either (I) when delivered personally to the Party for whom intended, (ii) upon delivery by an overnight courier service that is generally recognized as reliable, and the written records maintained by the courier shall be prima facie evidence of delivery, or (iii) on delivery (or attempted delivery) by certified or registered mail, return receipt requested, postage prepaid, as of the date shown by the return receipt; in any case addressed to such Party as set forth below or as a Party may designate by written notice given to the other Party in accordance herewith.

If to SMG: SMG
1950 Eisenhower Blvd.,
Fort Lauderdale, FL 33316 Attention:
Director of Operations

If to Provider: _____

Attention: _____

(d) Cooperation/Mediation.

- (i) The Parties desire to cooperate with each other in the performance of their respective duties pursuant to the terms of this Agreement. In keeping with this cooperative spirit and intent, any dispute arising hereunder, other than those necessary to preserve, protect, enforce, or defend the rights and/or obligations of either SMG and/or the Owner under the Management Agreement which shall be exempt from the mediation requirements of this Section **13(d)**, will first be referred to the Parties' respective agents or representatives prior to either Party initiating a legal suit, who will endeavor in good faith to resolve any such disputes within the limits of their authority and within thirty (30) days after the commencement of such discussions. If and only if any dispute remains unresolved after the parties have followed the dispute resolution procedure set forth above, the matter will be resolved pursuant to Sections **13(d)(ii)** and (iii) below.
- (ii) If any dispute between the Parties has not been resolved pursuant to Section **13(d)(I)** above, the Parties will endeavor to settle the dispute by mediation under the then current Center for Public Resources ("**CPR**") model procedure for mediation of business disputes or, if such model procedure no longer exists, some other mutually agreeable procedure. Within ten (10) business days from the date that the Parties cease direct negotiations pursuant to Section **13(d)(I)** above, SMG shall select a neutral third-party mediator, who shall be subject to the reasonable approval of Provider. Each Party will bear its own cost of mediation; provided, however, the cost charged by any independent third-party mediator will be shared equally by the Parties.
- (iii) The Parties agree that any mediation proceeding (as well as any discussion pursuant to Section **13(d)(I)** above) will constitute settlement negotiations for purposes of the federal and state rules of evidence and will be treated as non-discoverable, confidential, and privileged communication by the Parties and the mediator. No stenographic, visual, or audio record will be made of any mediation proceedings or such discussions. All conduct, statements, promises, offers, and opinions made in the course of the mediation or such discussion by any Party, its agents, employees, representatives, or other invitees and by the mediator will not be discoverable nor admissible for any purposes in any litigation or other proceeding involving the Parties and will not be disclosed to any third party.
- (iv) The Parties agree that this mediation procedure will be obligatory and participation therein legally binding upon each of them. In the event that Party refuses to adhere to the mediation procedure set forth in this Section **13(d)**, the

other Party may bring an action to seek enforcement of such obligation in any court of competent jurisdiction.

- (v) The Parties' efforts to reach a settlement of any dispute will continue until the conclusion of the mediation proceeding. The mediation proceeding will be concluded when: (I) a written settlement agreement is executed by the Parties; (ii) the mediator concludes and informs the Parties in writing that further efforts to mediate the dispute would not be useful; or (iii) the Parties agree in writing that an impasse has been reached. Notwithstanding the foregoing, either Party may withdraw from the mediation proceeding without liability therefore in the event such proceeding continues for more than forty-five (45) days from the commencement of such proceeding. For purposes of the preceding sentence, the proceeding will be deemed to have commenced following the completion of the selection of a mediator as provided in Section **13**(d)(ii).
- (vi) If any dispute has not been resolved pursuant to the foregoing, either Party can initiate litigation and/or terminate this Agreement as provided in Section 4(b) herein. The procedure specified in this Section **13**(d) shall be the sole and exclusive procedure for the resolution of disputes between the Parties arising out of or relating to this Agreement; provided, however, that a Party, without prejudice to the above procedures, may file a complaint to seek a preliminary injunction or other provisional judicial relief, if in its sole discretion such action is necessary to avoid irreparable damage or to preserve the status quo. Despite such action, the Parties will continue to participate in good faith in the procedures specified in this Section **13**(d).
- (vii) All applicable statutes of limitation and defenses based upon the passage of time shall be tolled while the procedures specified in this Section **13**(d) are pending. The Parties will take such action, if any, required to effectuate such tolling. Each Party shall be required to perform its obligations under this Agreement pending final resolution of any dispute arising out of or relating to this Agreement, unless to do so would be impossible or impracticable under the circumstances.
- (e) Force Majeure. Except as otherwise provided herein, neither Party shall be liable for any loss or delay resulting from any force majeure event, including, but not limited to, acts of God, fires, natural disaster, terrorism, epidemics/pandemics/public health emergencies, quarantine restrictions, labor stoppage, failure of public utilities, civil unrest, orders or directives of applicable federal, state, or local governmental entities (including, but not limited to Owner), or war or military hostilities, and any delivery or performance date shall be extended to the extent of any resulting delay.
- (f) Property of SMG. To the extent that any materials are developed or prepared by Provider in connection with the performance of its obligations hereunder, then such materials shall be deemed to be a part of this Agreement and shall be and remain the property of SMG at all times, notwithstanding the expiration or termination of this Agreement at any time for any reason.
- (g) Joint Preparation. This Agreement has been jointly prepared by the Parties and shall not be construed more strictly against either Party.
- (h) Priority of Provisions. If there is a conflict or inconsistency between any term, statement, requirement, or provision of any document or exhibit attached to, referenced by, or incorporated in this Agreement and any provision within an article

or section of this Agreement, the article or section shall prevail and be given effect.

- (i) Incorporation by Reference. The attached Exhibits are incorporated into and made a part of this Agreement.
- (j) Multiple Originals and Counterparts. This Agreement may be executed in multiple originals or in counterparts, whether signed physically or electronically; each of which shall be deemed to be an original, and all of which, taken together, shall constitute one and the same agreement.
- (k) Owner's Regulatory Authority/Capacity. Notwithstanding the fact that Owner is a political subdivision with certain regulatory authority, Owner's status as an express third-party beneficiary under this Agreement is not in its regulatory capacity. If Owner exercises its regulatory authority, the exercise of such authority and the enforcement of any rules, regulation, laws, and ordinances shall have occurred pursuant to Owner's regulatory authority as a governmental body separate and apart from this Agreement and shall not be attributable in any manner to Owner as a third-party beneficiary under this Agreement, nor impact any rights Owner may have as a third-party beneficiary.
- (l) Living Wage Requirement. If Provider is a "covered employer" within the meaning of the Broward County Living Wage Ordinance, Sections 26-100 through 26-105, Broward County Code of Ordinances, Provider shall fully comply with the requirements of such ordinance and shall pay to all of its employees providing "covered services," as defined in the ordinance, a living wage as defined therein. Provider shall ensure all of its subcontractors that qualify as "covered employers" fully comply with the requirements of such ordinance.

IN WITNESS WHEREOF, the Parties hereto have made and executed this Agreement: SMG, signing by and through its _____ duly authorized to execute same, and Provider, signing by and through its _____ duly authorized to execute same.

SMG

WITNESS:

SMG, a General Partnership

Signature

Authorized Signer

Print/Type Name

Print/Type Name & Title

_____ day of _____ 2026

_____ day of _____ 2026

Provider

(Insert Provider Name)

WITNESS:

Signature

Authorized Signer

Print/Type Name

Print/Type Name & Title

_____ day of _____ 2026

_____ day of _____ 2026

EXHIBIT A
DESCRIPTION OF SERVICES

THIS PAGE LEFT BLANK INTENTIONALLY WILL BE FILLED OUT UPON AWARD OF CONTRACT.

EXHIBIT B
PAYMENT SCHEDULE

THIS PAGE LEFT BLANK INTENTIONALLY WILL BE FILLED OUT UPON AWARD OF CONTRACT.

EXHIBIT C -- INSURANCE

- (a) A commercial general liability insurance policy in form acceptable to SMG including: (1) premises/operations, (2) products/completed operations liability, (3) property damage, (4) broad form contractual, and (5) personal injury, bodily injury and advertising injury. This general liability insurance shall have limits not less than:
 - a. \$1,000,000 each occurrence
 - b. \$1,000,000 general aggregate
- (b) Commercial automotive bodily injury and property damage insurance in form acceptable to SMG for business use covering all vehicles operated by Provider, its officers, agents, and employees in connection with the Services, whether owned by Provider, SMG, or otherwise, with a combined single limit of not less than One Million Dollars (\$1,000,000) (including an extension of hired and non-owned coverage);
- (c) Commercial umbrella liability insurance with a minimum limit of One Million Dollars (\$1,000,000) per occurrence; and,
- (d) Worker's Compensation insurance which meets applicable statutory limits including employer's liability with limits not less than:
 - a. \$100,000 bodily injury by accident – each accident
 - b. \$100,000 bodily injury by accident – each employee
 - c. \$500,000 bodily injury by disease – policy limit
- (e) The following shall apply to the insurance policies described in (a, b, c, and d) above:
 - a. Provider shall ensure that SMG and Owner are listed and endorsed as additional insureds on all policies required under this Exhibit C. At least thirty (30) days prior to the commencement of this Agreement, Provider shall provide SMG with a copy of all Certificates of Insurance or other documentation sufficient to demonstrate the insurance coverage required in this Exhibit C. Each such policy or certificate shall contain a valid provision or endorsement stating, "This policy will not be canceled or materially changed or altered without first giving thirty (30) days' written notice thereof to each of SMG, Risk Management Director, 300 Conshohocken State Rd., Suite 770, West Conshohocken, PA, 19428, and Broward County, Florida, 1950 Eisenhower Blvd, Ft Lauderdale, FL 33316." If any of the insurance policies covered by the foregoing Certificates of Insurance will expire prior to the expiration of this Agreement, Provider shall deliver to SMG at least thirty (30) days prior to such expiration a certificate of insurance evidencing the renewal of such policy or policies. If and to the extent requested by SMG, Provider shall provide, complete, certified copies of all required insurance policies and all required endorsements within thirty (30) days after SMG's request.
 - b. Provider shall ensure that all insurance coverages required by this Exhibit C remain in full force and effect without any lapse in coverage throughout the Term and until all performance required of Provider has been completed, as determined by SMG. Provider or its insurer shall provide notice to SMG of any

cancellation or modification of any required policy at least thirty (30) days prior to the effective date of cancellation or modification, and at least ten (10) days prior to the effective date of any cancellation due to nonpayment, and shall concurrently provide SMG with a copy of its updated Certificates of Insurance evidencing continuation of the required coverage(s).

- c. The coverage provided under such policies shall be occurrence-based, not claims made.
- d. Provider hereby acknowledges that the coverage limits contained in any policy, whether such limits are per occurrence or in the aggregate, shall in no way limit the liabilities or obligations of Provider under this Agreement, including, without limitation, Provider's indemnification obligations.
- e. All required insurance policies must be placed with insurers or surplus line carriers authorized to conduct business in the State of Florida with an A.M. Best rating of A- or better and a financial size category class VII or greater, unless otherwise approved by Owner's Risk Management Division in writing.
- f. If Provider maintains broader coverage or higher limits than the insurance requirements stated in Exhibit C, SMG and Owner shall be entitled to all such broader coverages and higher limits. All required insurance coverages shall provide primary coverage and not require contribution from any SMG or Owner insurance, self-insurance, or otherwise, which shall be in excess of and shall not contribute to the required insurance provided by Provider.
- g. Provider shall declare in writing any self-insured retentions or deductibles over the limit(s) prescribed in Exhibit C and submit to SMG for approval at least thirty (30) days prior to the commencement of this Agreement. Provider shall be solely responsible for and shall pay any deductible or self-insured retention applicable to any claim against Owner and SMG. SMG may, at any time, require Provider to purchase coverage with a lower retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. Any deductible or self-insured retention may be satisfied by either the named insured, Owner or SMG, if so elected by Owner and SMG, respectively, and Provider shall obtain same in endorsements to the required policies.
- h. Unless prohibited by the applicable policy, Provider waives any right to subrogation that any of Provider's insurers may acquire against Owner and SMG, and shall obtain same in an endorsement of Provider's insurance policies.
- i. If Provider or any subcontractor fails to maintain the insurance required by this Agreement, SMG may pay any costs of premiums necessary to maintain the required coverage and deduct such costs from any payment otherwise due to Provider. If requested by SMG, Provider shall provide, within one (1) business day, evidence of each subcontractor's compliance with the insurance requirements of this Agreement.

SCHEDULE 3: SMG's Contractor Safety Program

Safety Rules

These safety rules have been established for the protection of each team member. All team members are requested to cooperate in observing these rules and to help maintain a safe work environment. Team members should:

- Report all accidents and injuries to your Supervisor/Manager immediately, including near misses.
- Never operate any machine or equipment unless you are specifically authorized and trained to do so.
- Not operate defective equipment. Do not use broken hand tools. Report defective or hazardous equipment to your supervisor.
- Make sure all safety attachments are in place and properly adjusted before operating any machine.
- Not operate any machine or equipment at unsafe speeds or in an unsafe manner. Shut off equipment that is not in use.
- Wear all protective garments and equipment necessary to be safe. Wear proper shoes. Sandals or other open-toed or thin-soled shoes should not be worn.
- Never oil, clean, repair or adjust any machine while it is in motion and unless authorized to do so.
- Not lift items, which are too bulky or too heavy to be managed by one person. Ask for assistance.
- Keep all aisles, stairways, and exits clear of skids, boxes, air hoses, equipment, and spillage.
- Not place equipment and materials so as to block emergency exit routes, fireboxes, sprinkler shutoffs, machine or electrical control panels, or fire extinguishers.
- Stack all materials neatly and make sure piles are stable.
- Keep your work area, machinery, and all company facilities, neat and clean; Put tools and equipment away when they are not in use.
- Not participate in horseplay, teasing or otherwise distract fellow team members from the job they are doing.
- Safeguard other workers at all times.
- Not block emergency evacuation routes, fire extinguisher locations and eye wash station locations in your surrounding area.
- Keep all flammable liquids in approved containers and stored in appropriate cabinets.
- Never stand or work under a suspended load, be it hoist, crane or forklift.
- Always use a ladder instead of climbing on racks, materials, or crates.
- Smoke only in designated smoking areas.
- Company vehicles are to be driven by authorized team members only during Legends Global business hours.
- All team members are expected to wear seat belts at all times while in a moving vehicle being used for company business, whether they are the driver or a passenger.
- Use of handheld business phones, whether personal or business-owned, while behind the wheel of a moving vehicle being used on company business is strictly prohibited. It is every team member's responsibility to maintain a safe and clean work environment.

LOCATION CERTIFICATION FORM

Providers must circle one (1) from the following options.

The undersigned Provider hereby certifies that:

Option 1: The Provider has an office in Broward County. The Provider further certifies that:

- A.** It has continuously maintained,
 - i. a physical business address located within the limits of Broward County, listed on the Provider's valid business tax receipt issued by Broward County (unless exempt from business tax receipt requirements),
 - ii. in an area zoned for the conduct of such business,
 - iii. that the Provider owns or has the legal right to use, and
 - iv. from which the Provider operates and performs on a day-to-day basis business that is a substantial component of the goods or services being offered to Broward County in connection with this solicitation.

If Option 1 is selected, indicate the office location:

Option 2: The Provider has its corporate headquarters located in Broward County. The Provider further certifies that:

- B.** The Provider has continuously maintained,
 - i. a physical business address located within the limits of Broward County, listed on the Provider's valid business tax receipt issued by Broward County (unless exempt from business tax receipt requirements),
 - ii. in an area zoned for the conduct of such business,
 - iii. that the Provider owns or has the legal right to use, and
 - iv. from which the Provider operates and performs on a day-to-day basis business that is a substantial component of the goods or services being offered to Broward County in connection with this solicitation.
- C.** The corporate headquarters located in Broward County is the primary business address of the majority of the Provider's employees as of the bid posting date, and/or the majority of the work under the solicitations, if awarded to the Provider, will be performed by employees of the Provider whose primary business address in the corporate headquarters location in Broward County: and

D. The Provider's management directs, controls, and coordinates all or substantially all of the day- to-day activities of the entity (such as marketing, finance, accounting, human resources, payroll, and operations) from the corporate headquarters located in Broward County.

If Option 2 is selected, indicate the corporate headquarters location:

Option 3: The Provider does not have an office in Broward County, nor does it have a corporate headquarter located in Broward County.

If Option 3 is selected, indicate the office location:

Required Supporting Documentation (in addition to this form): Option 1 or 2:

1. Broward County Local business tax receipt.

AUTHORIZED SIGNATURE/NAME: _____

TITLE: _____

PROVIDER NAME: _____

DATE: _____

Parking Access & Revenue Control System
BCCC/SMG

Parking Access and Revenue Control System					
	Point Value	Vendor 1	Vendor 2	Vendor 3	Vendor 4
Pricing/Commission	20				
Points for price. Total points awarded for pricing will be determined by applying the following formula: (Lowest Proposed Cost / Proposer's Cost) x 20 = Price Score	20				
24/7 Customer Service & Technical Support	20				
Equipment and systems serviced directly by the Proposer versus third-party providers.	5				
Offline operational capabilities and transaction recovery procedures.	5				
Communication methods, estimated response times, and designated points of contact	5				
Service level agreements (SLAs) and uptime commitments	5				
Broward County Based Business	5 Max				
Option 1 - Office in Broward County (5)	3				
Option 2 - Corporate headquarters located in Broward County (2)	2				
Implementation & Transition	10				
Proposer's implementation approach, transition from gated to gateless operations, operational continuity, infrastructure protection, staff training, testing and validation, and ability to minimize disruption during installation and go-live activities.	10				
Revenue Protection and Capture Rate	15				
Evaluation of documented payment capture and compliance rates, LPR accuracy, revenue protection measures, collections integration, and demonstrated success in comparable gateless parking environments.	15				
Experience/History	10				
Experience with gateless PARCS systems, comparable high-volume facilities, successful project implementations, client references, financial stability, and overall performance history.	10				
Data Ownership & Security	15				
Proposer's data ownership, security, privacy, and PCI-DSS compliance practices including data storage, retention, backup, cybersecurity protections, and restrictions on the use or disclosure of County Data.	15				
Bid Submittal & Compliance	5				
Completeness, accuracy and responsiveness of bid submission, including compliance with all required submittals and documents identified in section 4.03	5				



Enterprise Technology Services Vendor Security Questionnaire (VSQ)

ETS Vendor Security Questionnaire (VSQ): Vendor is required to submit a completed ETS Vendor Security Questionnaire (VSQ) (for applicable solution – services, hardware, and/or software). If a response requires additional information, attach additional pages with the required additional information with the additional pages and information labeled to match the applicable question number. If not provided with the submittal, the Vendor must submit within three business days after the County's written request.

The Vendor Security Questionnaire (VSQ) assesses the Vendor's security policies and/or system protocol and to identify any potential security vulnerabilities. The County will review the Vendor's VSQ response; any identified security concerns will be disclosed to the Evaluation Committee. Unresolved security concerns shall be considered by the Evaluation Committee as part of its final evaluation and may affect the Vendor's evaluation.

As the Vendor's authorized representative, I attest that any and all statements, oral, written or otherwise, made in support of the Vendor's response, are accurate, true and correct. I also acknowledge that inaccurate, untruthful, or incorrect statements made in support of the Vendor's response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to PART XI of the Broward County Procurement Code.

Vendor Name:	
Vendor Type (Manufacturer, Reseller, Other? If Other, specify.):	
Vendor Contact Person's Name / Title / Email Address:	
Product Name / Description:	
Solicitation Number and Title (If applicable):	

For each applicable section, complete the matrix by using the dropdown option to select YES or NO. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. **Select "N/A" if a question within a given section is not applicable.**

SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT SERVICES /			
No.	Area	Question	Vendor Response
			YES/NO Comments
1		REQUIRED RESPONSE: Will your organization provide SOFTWARE-AS-A-SERVICE (SaaS) ? (e.g. Software-as-a-service/SaaS, application, website)	
2		REQUIRED RESPONSE: Will your organization provide HOSTING SERVICES ?	
3		REQUIRED RESPONSE: Will your organization provide APPLICATION DEVELOPMENT SERVICES ? (e.g. on-premise, mobile, web, or other custom code)	
4		REQUIRED RESPONSE: Will your organization provide MANAGED OR PROFESSIONAL SERVICES (UNSUPERVISED BY COUNTY PERSONNEL) ? (Note: "Managed or Professional Services" used herein refers to <u>unsupervised</u> (by County personnel) installation, configuration, consulting, maintenance or monitoring of County systems, applications or infrastructure related to your organization's proposed solution.)	
STOP: If you selected NO for Questions 1 through 4 above, PROCEED TO SECTION 2.			
5	Supporting Documentation (Upon County's request)	Provide the following:	
6		a) Workflow diagram of stored or transmitted information (for SaaS and Hosting Services only)	
7		b) Security / Network Architecture diagram (for SaaS and Hosting Services only)	
8		c) Secure Coding standard (for Application Development Services only)	
9		d) Application Security Program standard (for Application Development Services only)	
9	Audit Reporting Requirements	Does your organization have a current System and Organization Controls (SOC) 2, Type II report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy)? (Note: For any SaaS or hosted application, the SOC report should be for the organization or application specifically, not the datacenter only.)	
10	Payment Card Industry (PCI) environments - Applicable only if Organization or its proposed subcontractor processes or collects credit card information.	Does your organization have a current Payment Card Industry (PCI) certification (e.g., Attestation of Compliance (AOC), Self-Assessment Questionnaire (SAQ))?	
11		Will the product or solution process or collect credit card information?	
12		Does your organization maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to confidential County data?	
13	Electronic Protected Health Information (ePHI) - Applicable only if Organization has access to or will be hosting or storing County ePHI.	Has your organization had a Risk Assessment performed in the past five years by an external auditor in conjunction with the HIPAA Security rule?	
14		Does your organization maintain current HIPAA specific policies and procedures in conjunction with the HIPAA Security Rule?	
15		Does your organization have a designated HIPAA Security and Privacy Officer(s)?	
16		Does your organization provide HIPAA Security training to your employees at time of hire and at least annually thereafter?	
17	Roles & Responsibilities	Has your organization appointed a central point of contact for security coordination?	
18		Does your organization have an expected timeframe to respond to initial contact for security related issues? Provide timeframe.	
19		Does your organization define the priority level of an issue (e.g., minor vs. major, 0-4 scale, etc.)? Describe.	

20		Does your organization have an expected Service Level Agreement (SLA) to implement changes needed to fix security issues according to priority level? Describe.		
21	Federated Identity Management and Web Services Integration	Does your organization's product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory)? Describe.		
22		Does your organization use web services and/or data import/export functions (e.g., API, FTP)? Describe.		
23	External Parties	Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization?		
24		Does your organization have a Disaster Recovery and Continuity of Operations plan that includes third-party dependencies to ensure critical business functions can continue even during a major disruption?		
25		Does your organization outsource any aspect of the service to a third party?		
26		Does your organization utilize any off-shore resources for development? Provide location(s).		
27		Does your organization build the application in-house?		
28		Does your organization share customer data with or enable direct access by any third-party?		
29		Will any proposed subcontractors process, access, transmit or store any County data?		
30		Do all proposed subcontractors contractually comply with your organization's security standards for data processing?		
31		Does your organization regularly audit your critical vendors? Describe.		
32	Information Security Policy & Procedures	Does your organization have documented standard policies and procedures for security and compliance?		
33	Risk Assessment	Does your organization have a process that addresses: (a) the identification and measurement of potential risks with mitigating controls (measures taken to reduce risk), and (b) the acceptance or transfer (e.g. insurance policies, warranties, etc.) of the remaining (residual) risk after mitigation steps have been applied?		
34	Regulatory Compliance	Is the product or solution currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.		
35		Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)?		
36		Has your organization experienced a data breach within the past five years that legally required reporting under applicable law?		
37		Does your organization have procedures for preservation of electronic records and audit logs in case of litigation hold?		
38	During Employment – Training, Education & Awareness	Have employees and proposed subcontractors received formal information security awareness training? Provide frequency.		
39		Have your organization's security policies and procedures been communicated to your employees?		
40		Are periodic security reminders provided to your organization's employees?		
41	Background Checks	Does your organization perform background checks (e.g., credential verification, criminal history, credit history) to examine and assess an employee's or proposed subcontractor's work and criminal history?		
42		Are individuals who would have access to the County's data subjected to periodic follow-up background checks?		
43	Prior to Employment - Terms and Conditions of Employment	Are employees and proposed subcontractors required to sign a non-disclosure agreement and/or confidentiality form upon initial employment?		
44		If so, are employees and proposed subcontractors required to sign the non-disclosure agreement annually?		
45	Termination or Change in Employment	Does your organization require that all equipment of any terminated employee or subcontractor is returned and that their user ID is disabled in all systems and badges and/or keys are returned?		
46		Upon transfer, is existing access reviewed for relevance for employees and subcontractors?		
47	Secure Areas	Does your organization have effective physical access controls (e.g., door locks, badge /electronic key ID and access controls) in place that prevent unauthorized access to facilities and a facility security plan?		
48		Is a locked screensaver displayed on unattended workstations?		
49		Do personnel abide by a clean desk policy to remove and secure sensitive/confidential information from their workspace at the end of the work day?		
50		Does your organization have a contingency plan in place to handle emergency access to facilities?		
51		Are physical access controls authorized? Describe who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data.		
52		Are there policies and procedures to document repairs and modifications to physical components of the facility that are related to security?		

53		Are employees or subcontractors permitted access to customer environments from your physical locations only?		
54	Application and Information Access Control - Confidential System Isolation	Are systems and networks that host, process, and/or transfer confidential information "protected" (i.e., isolated, logically or physically separated) from other systems and/or networks?		
55		Are internal and external networks separated by firewalls with access policies and rules?		
56	Data Security	Are development and test environments separate from production environments to protect production applications from inadvertent changes or disruption?		
57		Does your organization apply database and application logical segregation of customer data?		
58		Is this a multi-tenant solution?		
59		Will County's data be co-mingled with data of any other customer?		
60		Does your organization provide a means to encrypt data at rest (e.g., AES)?		
61		Will County's data be processed, accessed, transmitted or stored through an off shore environment (e.g., outside continental U.S, Alaska, Hawaii)?		
62		Does your organization provide a means to encrypt County confidential information in transit? Describe controls that are in place to protect confidential information when transferred (e.g., encryption).		
63		Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g., firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, multi-tenancy, virtualization, shared storage, etc.)?		
64		Does your organization use email encryption to protect sensitive/confidential information when communicating with third parties (e.g., IT vendors)?		
65		Are employees permitted to work remotely from a facility not owned or leased by the organization?		
66		Are encrypted communications required for all remote connections?		
67		Does your organization use a secure VPN connection with third parties (e.g., IT vendors)?		
68		Does your organization have protections in place for ensuring secure remote access (e.g., up-to-date antivirus, posture assessment, VPN enforcement, split tunneling)?		
69		Is there a formal (documented, approved, published, communicated, and implemented) remote access policy?		
70		Can your organization restrict access to the solution to and from the County's network in a "deny all, permit by exception" configuration (i.e., whitelist County IP addresses only)?		
71	Audit Logging	Does the software or solution perform audit logging? Describe.		
72		Does the software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?		
73		Does the software track events for user activity (e.g., failed/successful logins, privileged access)? Describe.		
74	Vulnerability Assessment and Remediation	Does your organization perform periodic vulnerability scans on your IT systems, networks, and supporting security systems? Provide frequency.		
75		Are internal or proposed subcontractors vulnerability assessments automated?		
76		Does your organization have a security patch management cycle in place to address identified vulnerabilities?		
77		Does your organization provide disclosure of vulnerabilities found in your environment and remediation timelines?		
78		Does your organization notify customer of applicable patches?		
79	Security Monitoring	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (e.g., with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports)?		
80		Does your organization monitor your systems and networks for security events? Describe monitoring (e.g., server and networking equipment logs such as servers, routers, switches, wireless APs, monitored regularly).		
81		Does your organization periodically review system activity? Provide frequency.		
82	Identity & Access Management	Does your organization have a formal access authorization process based on "least privilege" (i.e. employees are granted the least amount of access possible to perform their assigned duties) and "need to know" (e.g., access permissions granted based upon the legitimate business need of the user to access the information, role-based permissions, limited access based on specific responsibilities, network access request form)?		
83		Are systems and applications configured to restrict access only to authorized individuals (e.g., use of unique IDs and passwords, minimum password length, password complexity, log-in history, lockout, password change, expiration)?		
84		Is there a list maintained of authorized users with general access and administrative access (e.g., active directory user lists within a confidential application, a spreadsheet of users, a human resources file)?		

85		Does your organization maintain a list of "accepted mobile devices" (e.g., smart phones, cell phones) and are these devices tracked and managed (e.g., Mobile Device Management)?		
86		Is a Data Loss Prevention (DLP) in place to prevent the unauthorized distribution of confidential information?		
87		Is software installation for desktops, laptops, and servers restricted to administrative users only?		
88		Does software or system have automatic logoff for session inactivity?		
89		Does your organization control and monitor access to application source code in a secure manner?		
90		Does your organization deny developers access to production environments, as well as to any environments containing customer data?		
91		Are user IDs for your system uniquely identifiable?		
92		Does your organization have any shared accounts? Describe.		
93		Will your organization allow remote access from proposed subcontractors to the County network, with immediate deactivation after use?		
94		Can service accounts be configured to run as non-privileged user (i.e., non-Domain Admin)?		
95		Is Multi-Factor Authentication (MFA) required for employees/contractors for remote access to production systems?		
96		Is Multi-Factor Authentication (MFA) included as a feature in the proposed system?		
97	Entitlement Reviews	Does your organization have a process to review user accounts and related access (e.g., manual process of reviewing system accounts to user accounts in AD for both users and privileged access, such as admins, developers, etc.)?		
98	Antivirus	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?		
99		Is this antivirus product centrally managed (e.g., monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? Explain your policies and procedures for management of antivirus software.		
100		Does your organization have a process for detecting and reporting malicious software?		
101	Network Defense and Host Intrusion Prevention Systems	Does your organization have any Intrusion Protection System (IPS) in place for your environment?		
102		Are employees prevented from using personally owned smart phones or mobile devices to connect to the organization's network?		
103	Media Handling	Does your organization have procedures to protect documents and computer media (e.g., tapes, disks, hard drives, etc.) from unauthorized disclosure, modification, removal, and destruction?		
104		Is confidential data encrypted when stored on laptop, desktop, server hard drive, flash drive, backup tape (i.e., data at rest)?		
105		Are backup archives stored externally / offsite from your facility?		
106	Secure Disposal	Are there security procedures (e.g., use of secure wiping, NIST 800-88, etc.) for the decommissioning (replacement) of IT equipment and IT storage devices that contain or process confidential information?		
107	Separation of Duties	Are duties separated (e.g., front desk duties separated from accounting, data analysts access separated from IT support), where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of your IT assets?		
108	Change Management	Do formal testing and change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability during patching activities, changes to the system, changes to the workstations and servers with appropriate testing, notification, and approval, etc.?		
109	Incident Management	In the event of a major security incident or data breach, do you provide the County a third-party digital forensics/incident report?		
110		Does your organization identify, respond to, and mitigate suspected or known security incidents (e.g., incident form completed as a response to each incident)?		
111		Does your organization have a formal incident response and data breach notification plan and team?		
112		Is evidence properly collected and maintained during the investigation of a security incident (e.g., employing chain of custody and other computer forensic methodologies that are monitored by internal and/or external parties)?		
113		Are incidents identified, investigated, and reported according to applicable legal requirements?		
114		Are incidents escalated and communicated? Describe.		
115		Do you have a contingency plan in place to handle emergency access to the proposed solution?		
116	Disaster Recovery Plan & Backups	Does your organization have a mechanism to back up critical IT systems and County data? Describe.		
117		Does your organization periodically test your backup/restoration plan by restoring from backup media?		
118		Does your organization have a disaster recovery plan?		
119		Are disaster recovery plans updated and tested at least annually?		
120		Do any single points of failure exist that would disrupt functionality of the proposed product or service?		

121	Product Security Development Lifecycle	Does your organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing)?		
122		Does your organization maintain an end-of-life-schedule for the proposed software product or solution?		
123		Is the product engineered as a multi-tier architecture design?		
124		Is any proposed product or service within three years of end of life?		
125	Crypto Materials and Key Management	Does your organization have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure?		
126	Secure Software Design/Testing	Is the software currently certified by any security standards? (e.g., OWASP, NIST). List standards.		
127		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
128		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
129		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
130		Does your organization remediate all vulnerabilities identified prior to production deployment?		
131		Is your organization outsourcing any aspect of the service to a third party?		
132		Is the product engineered as a multi-tier architecture design?		
133		Does your organization have capability to respond to and update product for any unforeseen new regulatory requirements?		
134	Application Development Services - This section is applicable only if Organization is providing Application Development Services (e.g. on-premise, mobile, web, or other custom code)	Does your organization's development and testing teams receive training specific to application security? Describe.		
135		Does your organization's development team use a development framework? List development languages and framework.		
136		Does your organization follow secure coding development standards?		
137		Does your organization have a security methodology for continuous maintenance of the application and applicable components?		
138		Does your organization review security at each phase of the software development life cycle?		
139		Does your organization use an industry standard methodology for conducting security testing? Describe.		
140		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
141		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
142		Does your organization use an independent third party for periodic security penetration testing?		
143		Does your organization perform peer code reviews on source code prior to production deployment?		
144		Does your organization remediate all vulnerabilities identified prior to production deployment?		
145		Is your organization outsourcing any aspect of the development to a third party?		
146		Will the County receive a copy of the source code?		
147	Generative Artificial Intelligence (GenAI) - Refers to artificial intelligence technology that can produce various types of content such as text, images, music, videos, code, etc., based on inputs or prompts to create derived synthetic content beyond analyzing or acting on existing data.	Is GenAI used as a component of or in the research, development, or production of this solution or service?		
148		Is GenAI used in any way to provide ongoing support to this system or solution (e.g., client chatbot for support requests)?		
149		Does the proposed product or solution use a GenAI model that was developed in house?		
150		Does the proposed product or solution use a GenAI model that was developed by a third party (e.g., ChatGPT)?		
151		Does this solution interface with a third-party GenAI product?		
152		Does this solution interface with any free or open source GenAI components?		
153		Does your organization have policies and procedures including governance, privacy and security implemented to validate information generated by the GenAI for accuracy?		
154		Is data labeling used to identify content generated by the GenAI product or solution?		
155		Are data sources (e.g., social media, news articles, scientific journals) used in the GenAI model verified to ensure content provided is accurate?		
156		Will County data be used to train or fine tune the GenAI model used in this solution?		
157		Does your organization have a standard in place to update data used in the GenAI model frequently (e.g., weekly, monthly, quarterly) to ensure data integrity?		
158		Does your organization have established copyright and authorized use for all data used to develop and operate the GenAI model to prevent copyright violations?		
159		Is PII information handled or stored by this GenAI solution?		
160		Will any County data be stored or accessed by the GenAI component?		

161		Does your organization perform continuous monitoring to detect GenAI model drift (i.e., degradation of model performance due to changes in data, or relationships between input and output variables)?		
162		Does your organization have security controls implemented to secure the confidentiality of data entered in the GenAI product or solution?		
163		Will the system continue to function if the GenAI service is not available?		
164		Does your organization have a procedure implemented to identify, manage, and mitigate GenAI risk?		
165		Does your organization perform security testing to identify GenAI specific security vulnerabilities (e.g., data poisoning, prompt injection, model exfiltration)?		
166		Are employees allowed to use GenAI technology from a personal device when conducting company business?		
167		Has a third party vendor risk assessment been performed on this GenAI solution?		
SECTION 2: SOFTWARE INSTALLED IN COUNTY'S NETWORK				
No.	Area	Question	YES/NO	Vendor Response Comments
1	REQUIRED RESPONSE: Will your organization provide SOFTWARE INSTALLED LOCALLY IN COUNTY NETWORK?			
STOP: If you selected NO for Question 1, PROCEED TO SECTION 3.				
2	Supporting Documentation (Upon County's request)	Provide the following: a) Hardware and Software requirements (i.e. Operating System, CPUs, RAM)		
3		b) Network connectivity requirements		
4	Reseller	Will your organization act as a reseller to provide software to the County? If so, provide manufacturer documentation regarding the security controls of the software and a secure configuration document.		
5	Software Installation Requirements	Can the application and service accounts used to run the application be configured to run as non-privileged users (e.g., non-Local Administrator rights)?		
6		Does software require admin rights to be installed? Describe the level of administrative access the software will need on the County domain.		
7		Is remote access required for installation and support? Describe.		
8		Can the software be installed on and operated in a virtualized environment?		
9	Third Party Software Requirements	Is third party software (e.g., Java, Adobe, Log4j) required to be installed or embedded within your software for it to work? Provide software and minimum version.		
10		Are you using any open source software components (e.g., no paid license) without paid product support? If so, list software components.		
11		Will the software remain compatible with all updates and new releases of required third party software?		
12	Secure Software Design/Testing	Is the software currently certified by any security standards? (e.g., PCI-DSS). Provide standards.		
13		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
14		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
15		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
16		Does your organization remediate all vulnerabilities identified prior to production deployment?		
17		Is your organization outsourcing any aspect of the service to a third party?		
18		Is the product engineered as a multi-tier architecture design?		
19		Does your organization have capability to respond to and update product for any unforeseen new regulatory requirements?		
20	Audit Logging	Does software or solution perform audit logging? Describe.		
21		Does software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?		
22		Does software have audit reporting capabilities (e.g., user activity, privileged access)? Describe.		
23	Security Updates/Patching	Does software have a security patch process? Describe your software security patch process, frequency of security patches and upgrade cycle releases.		
24		Does your organization support electronic delivery of digitally signed software and upgrades?		
25	Secure Configuration / Installation (i.e. PA-DSS configuration)	Does software allow for secure configuration and installation (e.g., OS hardening, disabling unnecessary services, antivirus compatibility)?		
26		Will software or solution process or collect credit card information?		
27	Confidential Data	Does product or solution process, store or transmit confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?		
28		Does software restrict confidential data (e.g., Social Security Number or Date of Birth) from being used as a primary identifier?		
29		Does software have documentation showing where all confidential data is stored in the application?		
30	Encryption	Does software support encryption of data in motion (e.g., SSL)?		

31		Does software support encryption of data at rest (e.g., column-level encryption, files)? List controls.		
32	Authentication	Does product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory, etc.)? Describe.		
33	Roles and Responsibilities	Does software provide role-based access control?		
34		Is a service account required for this software to run?		
35		If so, does the service account require admin rights?		
36	Product Security Development Lifecycle	Does organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing, etc.)?		
37		Does your organization maintain end-of-life-schedule for the software product?		
38		Is product or service within three years of end of life?		
39	Regulatory Compliance	Is the software or solution currently certified by any security standards (e.g., PCI-DSS, HIPAA)? Provide proof of compliance documentation.		
40	Generative Artificial Intelligence (GenAI) - Refers to artificial intelligence technology that can produce various types of content such as text, images, music, videos, code, etc., based on inputs or prompts to create derived synthetic content beyond analyzing or acting on existing data	Is GenAI used as a component of or in the research, development, or production of this solution or service?		
41		Is GenAI used in any way to provide ongoing support to this system or solution (e.g., client chatbot for support requests)?		
42		Does the proposed product or solution use a GenAI model that was developed in house?		
43		Does the proposed product or solution use a GenAI model that was developed by a third party (e.g., ChatGPT)?		
44		Does this solution interface with a third-party GenAI product?		
45		Does this solution interface with any free or open source GenAI components?		
46		Does your organization have policies and procedures including governance, privacy and security implemented to validate information generated by the GenAI for accuracy?		
47		Is data labeling used to identify content generated by the GenAI product or solution?		
48		Are data sources (e.g., social media, news articles, scientific journals) used in the GenAI model verified to ensure content provided is accurate?		
49		Will County data be used to train or fine tune the GenAI model used in this solution?		
50		Does your organization have a standard in place to update data used in the GenAI model frequently (e.g., weekly, monthly, quarterly) to ensure data integrity?		
51		Does your organization have established copyright and authorized use for all data used to develop and operate the GenAI model to prevent copyright violations?		
52		Is PII information handled or stored by this GenAI solution?		
53		Will any County data be stored or accessed by the GenAI component?		
54		Does your organization perform continuous monitoring to detect GenAI model drift (i.e., degradation of model performance due to changes in data, or relationships between input and output variables)?		
55		Does your organization have security controls implemented to secure the confidentiality of data entered in the GenAI product or solution?		
56		Will the system continue to function if the GenAI service is not available?		
57		Does your organization have a procedure implemented to identify, manage, and mitigate GenAI risk?		
58		Does your organization perform security testing to identify GenAI specific security vulnerabilities (e.g., data poisoning, prompt injection, model exfiltration)?		
59		Are employees allowed to use GenAI technology from a personal device when conducting company business?		
60		Has a third party vendor risk assessment been performed on this GenAI solution?		
SECTION 3: HARDWARE				
No.	Area	Description	Vendor Response	
			YES/NO	Comments
1	REQUIRED RESPONSE: Will your organization provide HARDWARE ?			
STOP: If you selected NO to Question 1, SKIP THIS SECTION.				
2	Reseller	Will your organization act as a reseller to provide hardware products to the County? If so, provide manufacturer documentation regarding the supply chain security controls around the hardware and a secure configuration document.		
3	Secure Hardware Design/Testing	Is the hardware currently certified by any security standards (e.g., NIST FIPS)?		
4		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
5		Does your organization use automated tools for security testing or code reviews to identify security vulnerabilities (e.g., brute force, injection, buffer overflows)?		
6		Does your organization perform security testing based on industry standards (e.g., OWASP Top 10, SANS Top 25)?		
7		Does your organization remediate all vulnerabilities identified prior to production deployment?		

8		Is your hardware scanned to detect any vulnerabilities or backdoors within the firmware (i.e., operating system, application code)?		
9		Is your firmware upgraded to remediate vulnerabilities? Provide frequency.		
10		If a new vulnerability is identified, is there a documented timeframe for updates/releases? Provide frequency.		
11		Do you implement security measures during the manufacturing of the hardware? Describe.		
12		Is your organization outsourcing any aspect of the service to a third party?		
13		Are there physical security features used to prevent tampering of the hardware? Identify features.		
14	Security Updates/Patching	Does the hardware have a security patch process? Describe your hardware security patch process, frequency of security patches and upgrade cycle releases.		
15		Are there contingencies where key third-party dependencies are concerned?		
16		Will your organization provide a Software Bill of Materials (SBOM) listing all the open-source and third-party components included in the hardware you will be supplying?		
17	Identity & Access Management	Are remote control features embedded for the manufacturer's support or ability to remotely access? Describe.		
18		Do backdoors exist that can lead to unauthorized access? Describe.		
19		Do default accounts exist? List all default accounts.		
20		Can default accounts and passwords be changed by Broward County?		
21		Can service accounts be configured to run as non-privileged user (i.e., non-Domain Admin)?		
22	Confidential Data	Does the product or solution collect confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?		
23	Roles and Responsibilities	Is a service account required for this hardware?		
24		If so, does the service account require admin rights?		
25	Product Security Development Lifecycle	Is an end-of-life schedule maintained for the hardware?		
26		Is any proposed product or service within three years of end of life?		
27	Media Handling	Does your organization have a secure data wipe and data destruction program for proper drive disposal (e.g., Certificate of destruction, electronic media purging)? Describe.		
28	Regulatory Compliance	Is the hardware currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.		
29		Will the product or solution process or collect credit card information?		
30		Does your organization have a process to identify new laws and regulations with IT security implications?		
31	Generative Artificial Intelligence (GenAI) - Refers to artificial intelligence technology that can produce various types of content such as text, images, music, videos, code, etc., based on inputs or prompts to create derived synthetic content beyond analyzing or acting on existing data.	Is GenAI used as a component of or in the research, development, or production of this solution or service?		
32		Is GenAI used in any way to provide ongoing support to this system or solution (e.g., client chatbot for support requests)?		
33		Does the proposed product or solution use a GenAI model that was developed in house?		
34		Does the proposed product or solution use a GenAI model that was developed by a third party (e.g., ChatGPT)?		
35		Does this solution interface with a third-party GenAI product?		
36		Does this solution interface with any free or open source GenAI components?		
37		Does your organization have policies and procedures including governance, privacy and security implemented to validate information generated by the GenAI for accuracy?		
38		Is data labeling used to identify content generated by the GenAI product or solution?		
39		Are data sources (e.g., social media, news articles, scientific journals) used in the GenAI model identified to ensure content provided is verifiable?		
40		Will County data be used to train or fine tune the GenAI model used in this solution?		
41		Does your organization have a standard in place to update data used in the GenAI model frequently (e.g., weekly, monthly, quarterly) to ensure data integrity?		
42		Does your organization have established copyright and authorized use for all data used to develop and operate the GenAI model to prevent copyright violations?		
43		Is PII information handled or stored by this GenAI solution?		
44		Will any County data be stored or accessed by the GenAI component?		
45		Does your organization perform continuous monitoring to detect GenAI model drift (i.e., degradation of model performance due to changes in data, or relationships between input and output variables)?		
46		Does your organization have security controls implemented to secure the confidentiality of data entered in the GenAI product or solution?		
47		Will the system continue to function if the GenAI service is not available?		
48		Does your organization have a procedure implemented to identify, manage, and mitigate GenAI risk?		

49		Does your organization perform security testing to identify GenAI specific security vulnerabilities (e.g., data poisoning, prompt injection, model exfiltration)?		
50		Are employees allowed to use GenAI technology from a personal device when conducting company business?		
51		Has a third party vendor risk assessment been performed on this GenAI solution?		