

CONTRACT MA-280-TBD
FOR
COMMON USE PASSENGER PROCESSING (CUPPS) AND
COMMON USE SELF SERVICE (CUSS) SYSTEMS
REPLACEMENT & SUPPORT SERVICES
BETWEEN
JOHN WAYNE AIRPORT
AND
(TBD)



**CONTRACT MA-280-(TBD)
BETWEEN
COUNTY OF ORANGE
AND
TBD
FOR
COMMON USE PASSENGER PROCESSING (CUPPS) AND COMMON USE SELF SERVICE
(CUSS) SYSTEMS REPLACEMENT & SUPPORT SERVICES**

This Contract MA-280-(TBD) for Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services (Contract) is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California (“County”), and TBD (Contractor), with County and Contractor sometimes referred to as Party or collectively as Parties.

ATTACHMENTS

This Contract is comprised of this document and the following Attachments, which are attached hereto and incorporated by reference into this Contract:

Attachment A – Scope of Work
Attachment B – Payment and Compensation
Attachment C - Staffing Plan
Attachment D - JWA SLR Requirements
Attachment E - JWA Disentanglement List

RECITALS

WHEREAS, Contractor and County are entering into this Contract for Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) System Replacement & Support Services under a firm fixed fee Contract; and,

WHEREAS, County solicited Contract for Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services as set forth herein, and Contractor represented that it is qualified to provide Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services to the County as further set forth here; and,

WHEREAS, Contractor agrees to provide Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services to the County as further set forth in the Scope of Work, attached hereto as Attachment A; and,

WHEREAS, County agrees to pay Contractor based on the schedule of fees set forth in Payment/Compensation, attached hereto as Attachment B; and,

WHEREAS, the County Board of Supervisors has authorized the Procurement Officer or designee to enter into a Contract for Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services with the Contractor; and,

NOW, THEREFORE, the Parties mutually agree as follows:

DEFINITIONS

DPA shall mean the Deputy Purchasing Agent assigned to this Contract

BIDS shall mean Baggage Information Display System

BHS shall mean Baggage Handling System

BRS shall mean Baggage Reconciliation System

BSM shall mean Baggage Source Message

CBP shall mean Customs and Border Protection

CMS shall mean Content Management System

CUPPS shall mean Common Use Passenger Processing System

CUSE shall mean Common User Service Environment

CUSS shall mean Common Use Self Service

DCS shall mean Departure Control System

DDC shall mean Direct Digital Control

FIDS shall mean Flight Information Display System

GIDS shall mean Gate Information Display System

IATA shall mean International Air Transport Association

JWA shall mean John Wayne Airport, County of Orange

LDCS shall mean Local Departure Control System

PM shall mean Project Manager

RMS shall mean Resource Management System

SLA shall mean Service Level Agreement

TSA shall mean Transportation Security Administration

VCD shall mean Virtual Design and Construction

ARTICLES

General Terms and Conditions:

- A. **Governing Law and Venue:** This Contract has been negotiated and executed in the state of California and shall be governed by and construed under the laws of the state of California. In the event of any legal action to enforce or interpret this Contract, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the parties specifically agree to waive any and all rights to request that an action be transferred for adjudication to another County.

- B. **Entire Contract:** This Contract contains the entire Contract between the parties with respect to the matters herein, and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing. Electronic acceptance of any additional terms, conditions or supplemental Contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County's Procurement Agent or designee.
- C. **Amendments:** No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the parties; no oral understanding or agreement not incorporated herein shall be binding on either of the parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.
- D. **Taxes:** Unless otherwise provided herein or by law, price quoted does not include California state sales or use tax. Out-of-state Contractors shall indicate California Board of Equalization permit number and sales permit number on invoices, if California sales tax is added and collectable. If no permit numbers are shown, sales tax will be deducted from payment. The Auditor-Controller will then pay use tax directly to the State of California in lieu of payment of sales tax to Contractor.
- E. **Delivery:** Time of delivery of commodities and services is of the essence in this Contract. County reserves the right to refuse any commodities and services and to cancel all or any part of the commodities not conforming to applicable specifications, drawings, samples or descriptions or services that do not conform to the prescribed scope of work. Acceptance of any part of the order for commodities shall not bind County to accept future shipments nor deprive it of the right to return commodities already accepted at Contractor's expense. Over shipments and under shipments of commodities shall be only as agreed to in writing by County. Delivery shall not be deemed to be complete until all commodities or services have actually been received and accepted in writing by County.
- F. **Acceptance Payment:** Unless otherwise agreed to in writing by County, 1) acceptance shall not be deemed complete unless in writing and until all the commodities/services have actually been received, inspected, and tested to the satisfaction of County, and 2) payment shall be made in arrears after satisfactory acceptance. In the event the Contractor is terminated for any reason, County shall immediately receive one/twelfth (1/12) of all prepaid development services (as listed in the Contract) fore each month or portion thereof remaining for the applicable Contract year as listed in this Contract.
- G. **Warranty:** Contractor expressly warrants that the commodities covered by this Contract are 1) free of liens or encumbrances, 2) merchantable and good for the ordinary purposes for which they are used, and 3) fit for the particular purpose for which they are intended. Acceptance of this order shall constitute an agreement upon Contractor's part to indemnify, defend and hold County and its indemnities as identified in the Insurance and Indemnification section, and as more fully described in the Insurance and Indemnification section harmless from liability, loss, damage and expense, including reasonable counsel fees, incurred or sustained by County by reason of the failure of the goods/services to conform to such warranties, faulty work performance, negligent or unlawful acts, and non-compliance with any applicable state or federal codes, ordinances, orders, or statutes, including the Occupational Safety and Health Act (OSHA) and the California Industrial Safety Act. Such remedies shall be in addition to any other remedies provided by law.

- H. **Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Contractor shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor warrants that any software as modified through services provided hereunder will not infringe upon or violate any patent, proprietary right, or trade secret right of any third party. Contractor agrees that, in accordance with the more specific requirement contained in the Insurance and Indemnification section, it shall indemnify, defend and hold County and County Indemnitees harmless from any and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, costs and expenses but not including attorney's fees.
- I. **Assignment:** The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the parties. Furthermore, neither the performance of this Contract nor any portion thereof may be assigned by Contractor without the express written consent of County. Any attempt by Contractor to assign the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract.
- J. **Civil Rights and Nondiscrimination:**
1. **Civil Rights:** Contractor attests that services provided shall be in accordance with the provisions of Title VI and Title VII of the Civil Rights Act of 1964, as amended, Section 504 of the Rehabilitation Act of 1973, as amended, the Age Discrimination Act of 1975 as amended, Title II of the Americans with Disabilities Act of 1990, and other applicable State and federal laws and regulations prohibiting discrimination on the basis of race, color, national origin, ethnic group identification, age, religion, marital status, sex or disability. In all its activities within the scope of its airport program, the Contractor agrees to comply with pertinent statutes, Executive Orders, and such rules as identified in Title VI List of Pertinent Nondiscrimination Acts and Authorities to ensure that no person shall, on the grounds of race, color, national origin (including limited English proficiency), creed, sex, age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance. This provision is in addition to that required by Title VI of the Civil Rights Act of 1964. The above provision binds the Contractor and subcontractors from the bid solicitation period through the completion of the contract.
 2. **Nondiscrimination:** In the performance of this Contract, Contractor agrees that it will comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 of the California Labor Code.
 3. **Compliance with Nondiscrimination Requirements:** During the performance of this contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor"), agrees to the extent required by law as follows:
 - a. **Compliance with Regulations:** The Contractor (hereinafter includes consultants) will comply with the Title VI List of Pertinent Nondiscrimination Acts and Authorities, as they may be amended from time to time, which are herein incorporated by reference and made a part of this contract.
 - b. **Nondiscrimination:** The Contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, national origin (including limited

- English proficiency), creed, sex, age, or disability in the selection and retention of subcontractors, including procurements of materials and leases of equipment. The Contractor will not participate directly or indirectly in the discrimination prohibited by the Nondiscrimination Acts and Authorities, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR part 21.
- c. **Solicitations for Subcontracts, including Procurements of Materials and Equipment:** In all solicitations, either by competitive bidding or negotiation made by the Contractor for work to be performed under a subcontract, including procurements of materials, or leases of equipment, each potential subcontractor or supplier will be notified by the Contractor of the contractor's obligations under this Contract and the Nondiscrimination Acts and Authorities on the grounds of race, color, or national origin.
 - d. **Information and Reports:** The Contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the Sponsor or the Federal Aviation Administration to be pertinent to ascertain compliance with such Nondiscrimination Acts and Authorities and instructions. Where any information required of a contractor is in the exclusive possession of another who fails or refuses to furnish the information, the Contractor will so certify to the Sponsor or the Federal Aviation Administration, as appropriate, and will set forth what efforts it has made to obtain the information.
 - e. **Sanctions for Noncompliance:** In the event of a Contractor's noncompliance with the nondiscrimination provisions of this contract, the Sponsor will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:
 - a. Withholding payments to the Contractor under the contract until the Contractor complies; and/or
 - b. Cancelling, terminating, or suspending a contract, in whole or in part.
 - f. **Incorporation of Provisions:** The Contractor will include paragraphs (a) through (f) in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations, and directives issued pursuant thereto. The Contractor will take action with respect to any subcontract or procurement as the Sponsor or the Federal Aviation Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the Contractor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the Contractor may request the Sponsor to enter into any litigation to protect the interests of the Sponsor. In addition, the Contractor may request the United States to enter into the litigation to protect the interests of the United States.

Upon request by the County, Contractor will provide a copy of each subcontract to demonstrate the above language has been inserted.

- 4. **Title VI List of Pertinent Nondiscrimination Acts and Authorities:** During the performance of this Contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor") agrees to comply to the extent required by law or as such provisions may be modified with the following nondiscrimination statutes and authorities; including but not limited to:

1. Title VI of the Civil Rights Act of 1964 (42 USC § 2000d *et seq.*, 78 stat. 252) (prohibits discrimination on the basis of race, color, national origin);
2. 49 CFR part 21 (Nondiscrimination in Federally-Assisted programs of the Department of Transportation—Effectuation of Title VI of the Civil Rights Act of 1964);
3. The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 USC § 4601) (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);
4. Section 504 of the Rehabilitation Act of 1973 (29 USC § 794 *et seq.*), as amended (prohibits discrimination on the basis of disability); and 49 CFR part 27 (Nondiscrimination on the Basis of Disability in Programs or Activities Receiving Federal Financial Assistance);
5. The Age Discrimination Act of 1975, as amended (42 USC § 6101 *et seq.*) (prohibits discrimination on the basis of age);
6. Airport and Airway Improvement Act of 1982 (49 USC § 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex);
7. The Civil Rights Restoration Act of 1987 (PL 100-259) (broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, the Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms “programs or activities” to include all of the programs or activities of the Federal-aid recipients, sub-recipients and contractors, whether such programs or activities are Federally funded or not);
8. Titles II and III of the Americans with Disabilities Act of 1990 (42 USC § 12101, *et seq.*), (prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities) as implemented by U.S. Department of Transportation regulations at 49 CFR parts 37 and 38;
9. The Federal Aviation Administration’s Nondiscrimination statute (49 USC § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);
10. Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations (ensures nondiscrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations); [rescinded January 20, 2025]
11. Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs [70 Fed. Reg. at 74087 (2005)]; [rescinded March 1, 2025]
12. Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 USC § 1681, *et seq.*).
13. Contractor is required to insert the above Title VI List of Pertinent Nondiscrimination Acts and Authorities into every subcontract at any tier. Upon request by the County, Contractor will provide a copy of each subcontract to demonstrate that the above language has been inserted.

5. **Civil Rights Training:** Upon request by the County, Contractor is required to disseminate and provide training materials and other information related to Title VI Civil Rights to its staff as specified by the County.
- K. **Termination:** In addition to any other remedies or rights it may have by law, County has the right to immediately terminate this Contract without penalty for cause or after 30 days' written notice without cause, unless otherwise specified. Cause shall be defined as any material breach of contract, any misrepresentation or fraud on the part of Contractor. Exercise by County of its right to terminate Contract shall relieve County of all further obligation.
- L. **Consent to Breach Not Waiver:** No term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.
- M. **Independent Contractor:** Contractor shall be considered an independent contractor and neither Contractor, its employees, nor anyone working under Contractor shall be considered an agent or an employee of County. Neither Contractor, its employees nor anyone working under Contractor shall qualify for workers' compensation or other fringe benefits of any kind through County.
- N. **Performance Warranty:** Contractor shall warrant all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction. Contractor shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other commodities/services furnished by Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workmanlike manner; shall furnish all necessary labor, supervision, machinery, equipment, materials, and supplies, shall at its sole expense obtain and maintain all permits and licenses required by public authorities, including those of County required in its governmental capacity, in connection with performance of the work. If permitted to subcontract, Contractor shall be fully responsible for all work performed by subcontractors.
- O. **General Insurance Requirements:** Prior to the provision of services under this Contract, the Contractor agrees to carry all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage current, provide Certificates of Insurance, and endorsements to the County during the entire term of this Contract.

Contractor shall ensure that all subcontractors performing work on behalf of Contractor pursuant to this Contract shall be covered under Contractor's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for Contractor. Contractor shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from Contractor under this Contract. It is the obligation of Contractor to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by Contractor through the entirety of this Contract for inspection by County representative(s) at any reasonable time.

All self-insured retentions (SIR)'s shall be clearly stated on the Certificate of Insurance. Any SIR in excess of Fifty Thousand Dollars \$50,000 shall specifically be approved by the County's Risk Manager, or designee. The County reserves the right to require current audited financial reports from Contractor. If Contractor is self-insured, Contractor will indemnify the County for any and all claims resulting or arising from Contractor's services in accordance with the indemnity provision stated in this contract.

If the Contractor fails to maintain insurance acceptable to the County for the full term of this Contract, the County may terminate this Contract.

Qualified Insurer

The policy or policies of insurance must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com**).

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

All insurance policies required by this Contract shall waive all rights of subrogation against the **County of Orange, its elected and appointed officials, officers, employees, and agents** when acting within the scope of their appointment or employment.

Contractor shall provide thirty (30) days prior written notice to the County of any policy cancellation or non-renewal and ten (10) days prior written notice where cancellation is due to non-payment of premium and provide a copy of the cancellation notice to County. Failure to provide written notice of cancellation may constitute a material breach of the Contract, upon which the County may suspend or terminate this Contract.

Insurance certificates should be forwarded to the agency/department address listed on the solicitation.

If the Contractor fails to provide the insurance certificates and endorsements within ten (10) days of notification by CEO/Procurement or the agency/department procurement division, award may be made to the next qualified vendor.

County expressly retains the right to require Contractor to increase or decrease insurance of any of the above insurance types throughout the term of this Contract. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

County shall notify Contractor in writing of changes in the insurance requirements. If Contractor does not provide acceptable Certificates of Insurance and endorsements to County incorporating such changes within thirty (30) days of receipt of such notice, this Contract may be in breach without further notice to Contractor, and County shall be entitled to all legal remedies.

The procuring of such required policy or policies of insurance shall not be construed to limit Contractor's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

The policy or policies of insurance maintained by the Contractor shall provide the minimum limits and coverage as set forth below

Commercial General Liability

Minimum limits and coverage: \$1,000,000 per occurrence; \$2,000,000 aggregate

Required Coverage Forms

The Commercial General Liability coverage shall be written on occurrence basis utilizing Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

Required Endorsements

The Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

- A. An Additional Insured endorsement using ISO form CG 20 26 04 13, or a form at least as broad naming the *County of Orange its elected and appointed officials, officers, employees, and agents* as Additional Insureds, or provide blanket coverage, which will state *As Required by Written Contract*.
- B. A primary non-contributory endorsement using ISO form CG 20 01 04 13, or a form at least as broad evidencing that the Contractor's insurance is primary, and any insurance or self-insurance maintained by the County shall be excess and non-contributing.

The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

Automobile Liability including coverage for owned or scheduled, non-owned and hired vehicles

Minimum limits and coverage: \$1,000,000 combined Single Limit each accident

Required Coverage Forms

The Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

Workers' Compensation

Minimum limits and coverage: Statutory

Required Endorsements

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the *County of Orange, its elected and appointed officials, officers, agents, and employees* or provide blanket coverage, which will state *As Required by Written Contract*.

Employers Liability Insurance

Minimum limits and coverage: \$1,000,000 per accident or disease

Network Security & Privacy Liability

Minimum limits and coverage: \$5,000,000 per claims-made

Required Endorsements

The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance:

- A. An Additional Insured endorsement naming the *County of Orange, its elected and appointed officials, officers, agents, and employees* as Additional Insureds for its vicarious liability.
- B. A primary and non-contributory endorsement evidencing that the Contractor's insurance is primary, and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

If Contractor's Network Security & Privacy Liability is a "Claims-Made" policy, Contractor shall agree to the following:

- A. The retroactive date must be shown and must be before the date of the contract or the beginning of the Contract services.
- B. Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of Contract services.
- C. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of earlier termination of the Contract.

Technology Errors & Omissions

Minimum limits and coverage: \$1,000,000 per claims-made; \$1,000,000 aggregate

Required Endorsements

If Contractor's Technology Errors & Omissions is a "Claims-Made" policy, Contractor shall agree to the following:

- A. The retroactive date must be shown and must be before the date of the contract or the beginning of the Contract services.
- B. Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of Contract services.
- C. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of earlier termination of the Contract.

Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow Form coverage.

- P. **Changes:** Contractor shall make no changes in the work or perform any additional work without County's specific written approval.
- Q. **Change of Ownership/Name, Litigation Status, Conflicts with County Interests:** Contractor agrees that if there is a change or transfer in ownership of Contractor's business prior to completion of this Contract, and the County agrees to an assignment of the Contract, the new owners shall be required under terms of sale or other transfer to assume Contractor's duties and obligations contained in this Contract and complete them to the satisfaction of the County.

County reserves the right to immediately terminate the Contract in the event the County determines that the assignee is not qualified or is otherwise unacceptable to the County for the provision of services under the Contract.

In addition, Contractor has the duty to notify the County in writing of any change in the Contractor's status with respect to name changes that do not require an assignment of the Contract. The Contractor is also obligated to notify the County in writing if the Contractor becomes a party to any litigation against the County, or a party to litigation that may reasonably affect the Contractor's performance

under the Contract, as well as any potential conflicts of interest between Contractor and County that may arise prior to or during the period of Contract performance. While Contractor will be required to provide this information without prompting from the County any time there is a change in Contractor's name, conflict of interest or litigation status, Contractor must also provide an update to the County of its status in these areas whenever requested by the County.

The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with County interests. In addition to the Contractor, this obligation shall apply to the Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. The Contractor's efforts shall include, but not be limited to establishing rules and procedures preventing its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers in the performance of their duties.

- R. **Force Majeure:** Contractor shall not be assessed with liquidated damages or unsatisfactory performance penalties during any delay beyond the time named for the performance of this Contract caused by any act of God, war, civil disorder, employment strike or other cause beyond its reasonable control, provided Contractor gives written notice of the cause of the delay to County within 36 hours of the start of the delay and Contractor avails himself of any available remedies.
- S. **Confidentiality:** Contractor agrees to maintain the confidentiality of all County and County-related records and information pursuant to all statutory laws relating to privacy and confidentiality that currently exist or exist at any time during the term of this Contract. All such records and information shall be considered confidential and kept confidential by Contractor and Contractor's staff, agents and employees.
- T. **Compliance with Laws:** Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by County. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of the Insurance and Indemnification section, Contractor agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws.
- Contractor shall remain in compliance and in good standing, maintaining current and active business entity and/or nonprofit registration status, with all applicable federal, state and local registration requirements at the time of execution of the contract through the duration of the term of the Contract, and shall provide annual confirmation of current and active status to County through the term of the Contract.
- U. **Freight:** Prior to County's express acceptance of delivery of products. Contractor assumes full responsibility for all transportation, transportation scheduling, packing, handling, insurance, and other services associated with delivery of all products deemed necessary under Contract.
- V. **Severability:** If any term, covenant, condition or provision of this Contract is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.

- W. **Attorney Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, each party shall bear their own attorney's fees, costs and expenses.
- X. **Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each party had been represented by experienced and knowledgeable independent legal counsel of their own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each party further acknowledges that they have not been influenced to any extent whatsoever in executing this Contract by any other party hereto or by any person representing them, or both. Accordingly, any rule or law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Contract against the party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to effect the purpose of the parties and this Contract.
- Y. **Employee Eligibility Verification:** Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. Contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against Contractor or County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract.
- Z. **Indemnification:** Contractor agrees to indemnify, defend with counsel approved in writing by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided by Contractor pursuant to this Contract. If judgment is entered against Contractor and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, Contractor and County agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment. Notwithstanding anything stated above, nothing contained herein shall relieve Contractor of any insurance requirements of obligations created elsewhere in this Contract.
- AA. **Audits/Inspections:** Contractor agrees to permit County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit will be confined to those matters connected with the performance of Contract including, but not limited to, the costs of administering Contract. County will provide reasonable notice of such an audit or inspection.

County reserves the right to audit and verify Contractor's records before final payment is made.

Contractor agrees to maintain such records for possible audit for a minimum of three years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Contractor agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right to County to audit records and interview staff of any subcontractor related to performance of this Contract.

Should Contractor cease to exist as a legal entity, Contractor's records pertaining to this Contract shall be forwarded to County's Project Manager.

BB. Contingency of Funds: Contractor acknowledges that funding or portions of funding for this Contract may be contingent upon state budget approval; receipt of funds from, and/or obligation of funds by, the state of California to County; and inclusion of sufficient funding for the services hereunder in the budget approved by County's Board of Supervisors for each fiscal year covered by this Contract. If such approval, funding or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Contract without penalty.

CC. Expenditure Limit: Contractor shall notify County of Orange assigned Deputy Procurement Agent in writing when the expenditures against Contract reach 75 percent of the dollar limit on Contract. County will not be responsible for any expenditure overruns and will not pay for work exceeding the dollar limit on Contract unless a change order to cover those costs has been issued.

DD. California Public Records Act: Contractor and County agree and acknowledge that all information and documents related to the award and performance of this Contract may be subject to disclosure pursuant to the California Public Records Act, California Government Code Section 7920.000 et seq. Contractor shall not respond to any California Public Records Act request directed at County; all responses shall be handled by County.

Additional Terms and Conditions

1. **Scope of Contract:** This Contract specifies contractual terms and conditions by which County will procure Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services from Contractor as further detailed in the Scope of Work, identified and incorporated herein by this reference as "Attachment A".
2. **Term of Contract:** This Contract shall commence upon execution of all necessary signatures and continue for three (3) calendar years from that date, unless otherwise terminated by County.
3. **Renewal:** This Contract may be renewed by mutual written agreement of both Parties for two (2) years. The County does not have to give reason if it elects not to renew. Renewal periods may be subject to approval by the County of Orange Board of Supervisors.
4. **Adjustments:** Scope of Work: No adjustments made to the Scope of Work will be authorized without prior written approval of County assigned Deputy Procurement Agent (DPA).
5. **Airport Security:** Contractor, Contractor's employees and Contractor's subcontractors must complete the following in order to obtain an Airport-Issued Security Identification Badge (ID Badge).
 - A. **Airport-Issued Badge Acquisition, Retention, and Termination:** Prior to issuance of airport security ID Badge(s), designated Contractor personnel who shall be working on-site in JWA restricted areas, and engaged in the performance of work under this Contract must pass JWA's security screening

requirements, which include fingerprinting to complete an F.B.I. Criminal History Records Check (CHRC) and a Security Threat Assessment (STA). Contractor should anticipate four to six weeks for new employees to receive an airport security ID badge which includes the following general steps:

1. Company designates at least two representatives as Authorized Signatories by submitting a letter on company letterhead using the airport's template.
2. Subcontractors and tenant contractors must also have two Authorized Signatories at a minimum.
3. All company employees requiring unescorted access to restricted airport areas are scheduled for fingerprint appointments.
4. Background check fees are provided at the first appointment.
5. Employees must provide two government-issued IDs at the first appointment.
6. STA and/or CHRC results are received.
7. All ID Badge applicants successfully passing the STA and/or CHRC are scheduled for required training.
8. ID Badge related fees are provided and any additional information requested is provided at the training appointment.
9. Upon successful completion of the required training, employees will receive their ID Badge.
10. Authorized Signatories are required to maintain the ID Badge process for the onboarding of future employees, employee ID Badge renewals, scheduling, and other actions detailed below.

Contractor's designated personnel must, at a minimum, complete the following required training based on contractors work to be provided and access areas:

1. Authorized Signatory Training: All organizations must designate at least two Authorized Signatories by providing a letter on company letterhead using the ID/Access Control Office template. The designated Authorized Signatories will be responsible for the entire ID Badge process for their organization including, but not limited to, the onboarding of new employees, renewing employees, scheduling employees for appointments, payment coordination, ID Badge audits, resolution to safety/security violations caused by the organizations employees, subtenants, or subcontractors. Authorized Signatories must attend this approximate 1 hour course initially and annually.
2. Security Identification Display Area (SIDA) Training: All employees with an operational need to have unescorted access to the Airport SIDA must complete this approximate 1.5 hour course and pass a written test.
3. Sterile Area (Elevator) Training: All Non-SIDA employees with an operational need to have unescorted access to the Sterile Area of the terminal must complete an approximate 30-minute training session and pass a written test.
4. Non-Movement Area or Movement Area Driver Training: All employees with an operational need to drive on airfield service roads and/or ramps must attend the approximate 1-hour Non-Movement Area Driver course and pass a written test. Employees with an operational need to drive on active taxiways and/or active runways must coordinate this training with the Airport Operations Division.

5. Contractors' designated personnel must successfully complete the badge acquisition within six weeks of Contract execution, unless other arrangements have been coordinated by County Project Manager or designee in writing.
 6. All personnel assigned to this contract must be in possession of a current, valid Airport-Issued ID Badge prior to fulfilling an independent shift assignment.
 7. Contractor is responsible for terminating and retrieving Airport-Issued ID Badges as soon as an employee no longer needs unescorted access to airport restricted areas. Terminated ID Badges must be returned to the ID/Access Control office within three business days. Failure to do so will result in a \$250.00 fee.
 8. Contractor shall be responsible for all cost associated with the Airport-Issued ID Badge process. The ID/Access Control Office maintains the current list of fees. Below is a list of estimated costs for new ID Badge applications and ID Badge renewals:
 - STA Fee: Approximately \$11.00
 - Fingerprint/CHRC Fee: Approximately \$31.00
 - ID Badge Fee: Approximately \$10.00
 - Terminated, Unreturned ID Badge Fee: Approximately \$250.00
 9. Contractor shall abide by all the security requirements set forth by the Transportation Security Agency (TSA) and JWA.
- B. Airport Driving Endorsement:** In addition to obtaining a JWA access control badge, Contractor's service staff with an operational need to drive on airport service roads and ramps must also take an Airport provided training course and pass a test to acquire an airfield driving endorsement.
- Some Air Operations Area projects will require vehicles to be equipped with visible company placards on both sides of the vehicle, an orange/white checkered flag, an amber, rotating beacon, and a two-way radio to monitor FAA Air Traffic Control Tower frequencies; or be escorted by a vehicle with this equipment and markings. Only vehicles, equipment, and personnel who have prior authorization by the ASP may operate on runways, taxiways and movement areas, or cross runways and taxiways. Under no circumstance shall any vehicle operate on or cross a runway, taxiway, or any movement area unless permission from the Tower is granted. Vehicles requiring an escort must be escorted by Airport Operations, or authorized company vehicles, equipped with two-way radios, and in constant radio communication with the FAA Tower Control.
- C. Airport ID Badge Holder Requirements and Responsibilities:** TSA approved security program for JWA requires that each person issued a JWA security badge is made aware of his/her responsibilities regarding the privilege of access to restricted areas of JWA.
1. All persons within the restricted air operation areas of JWA are required to display, on their person, a JWA security badge; unless they are specifically exempted for safety reasons or they are under escort by a properly badged individual. Each JWA employee, JWA Contractor, subcontractor or tenant employee who has been issued a JWA security badge is responsible for challenging any individual who is not properly displaying a JWA issued or approved and valid identification badge. Any person who is not properly displaying or who cannot produce a valid JWA security badge must immediately be referred to the Sheriff's Department - Airport Police Services Office for proper handling.

2. JWA security badge is the property of County and must be returned upon termination of Contractor personnel employment and/or termination, expiration or completion of Contract. The loss of a badge shall be reported within 24 hours to the Sheriff's Department - Airport Police Services by calling (949) 252-5000. Individuals that lose their badge shall be required to pay a fee before receiving a replacement badge. The charge for lost badge replacement shall be at the current posted rate located in the JWA Administration Office. A report shall be made before a replacement badge shall be issued.
 3. JWA security badge is nontransferable.
 4. In the event that a contractor's badge is not returned to JWA upon termination of Contractor personnel employment and/or termination or expiration of Contract, a fine of \$250.00 per badge shall be charged to Contractor. Contractor's final payment may be held by County or a deduction from contractor's payment(s) may be made to ensure that funding is available to cover the fine in the event that badges are not returned.
 5. Contractor shall submit the names, addresses, and driver's license numbers for all Contractor personnel who shall be engaged in work under this Contract to County Project Manager within seven days after award of the Contract or within seven days after the start of any new Contractor personnel and/or prior to the start of any work.
 6. No worker shall be used in performance of this work that has not passed the background check.
6. **Amendments – Changes/Extra Work:** The Contractor shall make no changes to this Contract without the County's written consent. In the event that there are new or unforeseen requirements, the County with the Contractor's concurrence has the discretion to request official changes at any time without changing the intent of this Contract.
- If County-initiated changes or changes in laws or government regulations affect price, the Contractor's ability to deliver services, or the project schedule, the Contractor shall give the County written notice no later than seven calendar days from the date the law or regulation went into effect or the date the change was proposed by the County and the Contractor was notified of the change. Such changes shall be agreed to in writing and incorporated into a Contract amendment. Said amendment shall be issued by the County assigned Deputy Purchasing Agent, shall require the mutual consent of all parties, and may be subject to approval by the County Board of Supervisors. Nothing herein shall prohibit the Contractor from proceeding with the work as set forth in this Contract.
7. **Americans with Disabilities Act (ADA):** Contractor shall comply with Section 504 of the Rehabilitation Act of 1973 as amended; Title VI and VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act, 42 USC 12101 et seq; California Code of Regulations, Title 2, Title 22: California Government Code, Sections 11135, et seq; and other federal and state laws and executive orders prohibit discrimination. All programs, activities, employment opportunities, and services must be made available to all persons, including persons with disabilities.
 8. **Anti-Idling Policy:** Within six months of Contract execution, Contractor must develop, implement and submit to the Airport Director for approval a fleet-wide anti-idling policy. At a minimum, the anti-idling policy shall include the requirement that vehicle engines shall be turned off when vehicles are not occupied, and that occupied vehicles be turned off after no more than a five-minute idling period. Contractor's policy shall also include all third-party vehicles that enter Airport property at the direction of Contractor.

9. **Bond Requirements:** Contractor shall furnish a Faithful Performance Bond and a Labor and Material Payment Bond, each in an amount equal to 100% percent of the Contract annual amount.
- A. Faithful Performance Bond: Contractor will provide to County a Faithfull Performance Bond in an amount equal to 100% percent of the annual Contract amount. Bond must be submitted to County on County provided forms within seven (7) calendar days of award notification and prior to the official Contract award. Prior to the provisions of services under this Contract, Contractor agrees to purchase the required bond at Contractor's expense and to deposit with County the required bond necessary to satisfy County requirements and to keep such bond on deposit with County during the entire term of this Contract. Said bond shall be secured from an admitted surety company authorized to conduct surety insurance in California and satisfactory to County Offices of County Counsel and Risk Management and in accordance with General Conditions.
 - B. Labor and Material Payment Bond: Contractor will provide to County a Labor and Material Payment Bond to guarantee payment of claims of labors, mechanics, material man, and other persons as set forth by law. Said bond shall be for one hundred percent (100%) of the **annual** Contract amount. Bond must be submitted to County on County provided forms within seven (7) calendar days of award notification and prior to the official Contract award. Prior to the provisions of services under this Contract, Contractor agrees to purchase the required bond at Contractor's expense and to deposit with County the required bond necessary to satisfy County requirements and to keep such bond on deposit with County during the entire term of this Contract. Said bond shall be secured from an admitted surety company authorized to conduct surety insurance in California and satisfactory to County Offices of County Counsel and Risk Management and in accordance with General Conditions
 - C. If any surety upon any bond furnished in connection with this Contract becomes unacceptable to County, or if any such surety fails to furnish reports as to its financial condition from time to time as requested by County, Contractor shall promptly furnish such additional security as may be required by County from time to time to protect the interests of the County and of persons supplying labor or material in the prosecution of the work contemplated by this Contract. No further payment shall be deemed due or shall be made under Contract until a new surety and/or bond is furnished to County.
County shall return bonds to Contractor after successful completion of all Contractor's obligations and services required under the Contract.
10. **Bills and Liens:** Contractor shall pay promptly all indebtedness for labor, materials and equipment used in performance of the work. Contractor shall not permit any lien or charge to attach to the work or the premises, but if any does so attach, Contractor shall promptly procure its release and, in accordance with the requirements of Article "Indemnification" above, indemnify, defend, and hold County harmless and be responsible for payment of all costs, damages, penalties and expenses related to or arising from or related thereto.
11. **Breach of Contract:** The failure of Contractor to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:
- A. Terminate Contract immediately, pursuant to the General Terms and Conditions section, "Termination" Article herein;
 - B. Afford Contractor written notice of the breach and ten (10) calendar days or such shorter time that may be specified in this Contract within which to cure the breach;

- C. Discontinue payment to the Contactor for and during the period in which Contractor is in breach; and
- D. Offset against any monies billed by the Contractor but yet unpaid by the County those monies disallowed pursuant above.

12. **Conditions Affecting Work:** Contractor shall be responsible for taking all steps reasonably necessary to ascertain the nature and location of the work to be performed under this Contract and to know the general conditions which can affect the work or the cost thereof. Any failure by Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to County. County assumes no responsibility for any understanding or representations concerning the nature, location(s) or general conditions made by any of its officers or agents prior to the execution of this Contract, unless such understanding or representations by County are expressly stated in Contract.

13. **Conflict of Interest – Contractor’s Personnel:** Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to Contractor; the Contractor’s officers, directors, employees, agents, and subcontractors associated with accomplishing work and services hereunder. Contractor’s efforts shall include, but not be limited to establishing precautions to prevent its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers from acting in the best interests of the County.

Contractor shall notify County, in writing, of any potential or actual conflicts of interest between Contractor and County that may arise prior to, or during the period of, Contract performance, including, but not limited to, whether any known County public officer’s child is an officer or director of, or has an ownership interest of ten (10) percent or more in, Contractor. While Contractor will be required to provide this information without prompting from County any time there is a change regarding conflict of interest, Contractor must also provide an update to County upon request by County.

14. **Conflict of Interest County Personnel:** County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. Contractor shall not, during the period of this Contract, employ any County employee for any purpose.

15. **Contractor’s Project Manager and Key Personnel:** Contractor shall appoint a Project Manager to direct Contractor’s efforts in fulfilling Contractor’s obligations under this Contract. This Project Manager shall be subject to approval by County and shall not be changed without the written consent of County’s Project Manager, which consent shall not be unreasonably withheld.

Contractor’s Project Manager shall be assigned to this project for the duration of Contract and shall diligently pursue all work and services to meet the project timelines. County’s Project Manager shall have the right to require the removal and replacement of Contractor’s Project Manager from providing services to County under this Contract. County’s Project manager shall notify Contractor in writing of such action. Contractor shall accomplish the removal within five (5) business days after written notice by County’s Project Manager. County’s Project Manager shall review and approve the appointment of the replacement for Contractor’s Project Manager. County is not required to provide any additional information, reason or rationale in the event it requires the removal of Contractor’s Project Manager from providing further services under Contract,

16. **Contractor Personnel – Reference Checks:** Contractor warrants that all persons employed to provide service under this Contract have satisfactory past work records indicating their ability to adequately perform the work under this Contract. Contractor’s employees assigned to this project must meet character standards as demonstrated by background investigation and reference checks, coordinated by the agency/department issuing this Contract.
17. **Contractor Personnel – Uniform/Badges/Identification:** Contractor warrants that all persons employed to provide service under this Contract have satisfactory past work records indicating their ability to accept the kind of responsibility under this Contract. All Contractor’s employees shall be required to wear uniforms, badges, or other means of identification which are to be furnished by Contractor and must be worn at all times while working on County property. The assigned Deputy Procurement Agent must be notified in writing, within seven (7) days of notification of award of Contract of the uniform and/or badges and/or other identification to be worn by employees prior to beginning work and notified in writing seven (7) days prior to any changes in this procedure.
18. **Contractor’s Records:** Contractor shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by Contractor in accordance with generally accepted accounting principles. These records shall be stored in Orange County for a period of three (3) years after final payment is received from County. Storage of records in another county will require written approval from County of Orange assigned Deputy Procurement Agent.
19. **Contractor Safety:** Contractor shall comply with the County’s Safety and Loss Prevention Policy and Procedure#306 (“Contractor Safety Responsibilities”) and submit a copy of their Injury and Illness Prevention Program (IIPP) and Contractor Safety-Activity Checklist to the County’s Project Manager prior to the start of any work performed under the Contract. Contractor will notify County Project Manager of any revisions to the Safety-Activity Checklist and will provide a new Safety-Activity Checklist upon County request. The IIPP shall comply with California Code of Regulations, Title 8, Section 1509 or 3203(whichever applies). Contractor shall submit other safety programs that pertain to the type of job that will be performed on site. County reserves the right to conduct inspections and audits as necessary for the purpose of evaluating any aspect of safety performance under this Contract.
20. **Cooperative Contract:** This Contract is a cooperative contract and may be utilized by all County of Orange departments.

The provisions and pricing of this Contract may be extended, at the option of Contractor, to any Municipal, County, Public Utility, Hospital, Educational Institution, or any other non-profit or governmental organization (the “Cooperative Program”). Parties in a Cooperative Program wishing to use this Contract will be responsible for issuing their own purchase documents / price agreements, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any agreement entered into with another agency or entity that is entered into pursuant to the provisions and pricing of this Contract a clause that binds the parties to the agreement to “indemnify, defend with counsel approved in writing by the County of Orange, California (“County”), and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County’s Board of Supervisors acts as the governing Board (“County Indemnitees”) harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided” under the agreement.. Failure to so include this clause voids the Contract’s extension to a Cooperative Program and will be considered a material breach of this Contract and grounds for immediate Contract termination. The cooperative entities are responsible for obtaining all

certificates of insurance and bonds required. The County of Orange makes no guarantee of usage by other users of this Contract.

As a cost-recovery mechanism for County, a 2 percent administrative rebate on total sales from all subordinate contracts will be paid to the County for any contracts the Contractor agrees to enter into with another agency or entity, other than the County of Orange or a department thereof, under the provisions and pricing of this Contract. The County has partnered with Pavilion, a third-party administrator, responsible for managing all reporting and payments under this Cooperative Program. The Contractor shall provide quarterly Volume Sales Reports about additional sales to other entities under the provisions and pricing of this Contract. The Reports shall include the ordering agency, detail of items sold including description, quantity, and price, and shall include all transactions pertaining to sales under the Contract provisions and pricing for that Reporting Period. Contractor shall provide the Volume Sales Reports regardless of whether or not any sales have been conducted. Failure of the Contractor to provide quarterly reports as required may be deemed by the County as a material breach of the Contract. A late penalty of 15 percent on the value of the rebate may be assessed to the Contractor for each month the payments are not received.

Subordinate contracts must be executed prior to the expiration or earlier termination of this Contract and may survive the expiration of this Contract. This Cooperative Contract provision shall survive expiration or termination of this Contract.

21. County Branding Requirement - Publicity, Literature, Advertisements and Social Media:

- A. County owns all rights to the name, logos, and symbols of County. The use/and/or reproduction of County's name, logos, or symbols for any purpose, including commercial advertisement, promotional purposes, announcements, displays, or press releases, without County's prior written consent is expressly prohibited.
- B. Contractor may develop and publish information related to this Contract where all of the following conditions are satisfied:
 1. Administrator/assigned Deputy Purchasing Agent provides its written approval of the content and publication of the information at least 30 days prior to Contractor publishing the information, unless a different timeframe for approval is agreed upon to the Administrator/assigned Deputy Purchasing Agent;
 2. Unless directed otherwise by Administrator/assigned Deputy Purchasing Agent, the information includes a statement that the program, wholly or in part, is funded through County, State and Federal government funds [funds identified as applicable];
 3. The information does not give the appearance that the County, its officers, or employees or agencies endorse:
 - a. any commercial product or service; and,
 - b. any product or service provided by Contractor, unless approved in writing by Administrator/assigned Deputy Purchasing Agent; and,
 4. If Contractor uses social media (such as Facebook, X platform, Instagram, YouTube or other publicly available social media sites) to publish information related to this Contract, Contractor shall develop social media policies and procedures and have them available to the Administrator/assigned Deputy Purchasing Agent. Contractor shall comply with County

Social Media Use Policy and Procedures as they pertain to any social media developed in support of the services described within this Contract. The policy is available on the Internet at <http://www.ocgov.com/gov/ceo/cio/govpolicies>.

24. **County of Orange Local Small Business Preference Requirements:** (Applicable only if Preference is Elected) Contractor certifies it is in compliance with the applicable County of Orange Local Small Business (OCLSB) and Disabled Veteran Business Enterprise (DVBE) Preference requirements at the time of bid/proposal submittal.
- If applicable, Contractor further certifies that any OCLSB and/or DVBE Subcontractor(s) specified in Attachment “Staffing Plan” comply with County’s OCLSB and/or DVBE Preference at the time of bid/proposal submittal and shall ensure that at least 20% of the Contract amount is allocated to OCLSB and/or DVBE Subcontractor(s) as specified in Attachment.
- For Public Works contracts, if applicable, Contractor shall ensure that at least 3% of any Contract amount expected to exceed five million dollars is allocated to OCLSB and/or DVBE Subcontractor(s), as specified in Attachment “Staffing Plan”.
25. **Disabled Veteran Business Enterprise Preference Requirements:** Contractor certifies it is in compliance with County of Orange Disabled Veteran Business Enterprise Preference requirements at the time this Contract is executed.
26. **Data – Title To:** All materials, documents, data or information obtained from County data files or any County medium furnished to Contractor in the performance of this Contract will at all times remain the property of County. Such data or information may not be used or copied for direct or indirect use by Contractor after completion or termination of this Contract without the express written consent of County. All materials, documents, data or information, including copies, must be returned to County at the end of this Contract.
27. **Default – Re-Procurement Costs:** In case of Contract breach by Contractor, resulting in termination by County, County may procure the commodities and services from other sources. If the cost for those commodities and services is higher than under the terms of the existing Contract, Contractor will be responsible for paying County the difference between Contract cost and the price paid, and County may deduct this cost from any unpaid balance due Contractor. The price paid by County shall be the prevailing market price at the time such purchase is made. This is in addition to any other remedies available under this Contract and under law.
28. **Department of the Treasury, Internal Revenue Service Form W-9 Requirement:** Effective June 3, 2006, all Contractors, entering into a contract with the County, who are not already established in the County Financial System as an Auditor-Controller Vendor, will be required to submit to the County a federal Form W-9, or form W-8 for foreign vendors. The County will inform the Contractor, at the time of award, if the Form W-9, or W-8, will be required.
- A. In order to comply with this County requirement, within ten days of notification of selection of award of Contract but prior to official award of Contract, the selected Contractor agrees to furnish to the contract administrator, the County DPA, the required W-9 or W-8. *Out of State Vendors may be required to submit a 587/590 Form.*

29. **Disputes – Contract:** The parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute concerning a question of fact arising under the terms of this Contract is not disposed of in a reasonable period of time by the Contractor's Project Manager and the County's Project Manager, as specified in Article titled "Notices" below, such matter shall be brought to the attention of the County DPA by way of the following process:

- A. The Contractor shall submit to the agency/department assigned Deputy Procurement Agent a written demand for a final decision regarding the disposition of any dispute between the parties arising under, related to, or involving this Contract, unless County, on its own initiative, has already rendered such a final decision.
- B. The Contractor's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to Contract, Contractor shall include with the demand a written statement signed by a senior official indicating that the demand is made in good faith, that the supporting data are accurate and complete, and that the amount requested accurately reflects Contract adjustment for which Contractor believes County is liable.

Pending the final resolution of any dispute arising under, related to, or involving this Contract, Contractor agrees to diligently proceed with the performance of this Contract, including the delivery of commodities and/or provision of services. Contractor's failure to diligently proceed shall be considered a material breach of this Contract.

Any final decision of County shall be expressly identified as such, shall be in writing, and shall be signed by County Deputy Procurement Agent or his designee. If County fails to render a decision within 90 days after receipt of Contractor's demand, it shall be deemed a final decision adverse to Contractor's contentions. Nothing in this section shall be construed as affecting County's right to terminate Contract for cause or termination for convenience as stated in Article "Termination" herein.

30. **Drug-Free Workplace:** Contractor hereby certifies compliance with Government Code Section 8355 in matters relating to providing a drug-free workplace. Contractor will:

- A. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a)(1).
- B. Establish a drug-free awareness program as required by Government Code Section 8355(a)(2) to inform employees about all of the following:
 1. The dangers of drug abuse in the workplace;
 2. The organization's policy of maintaining a drug-free workplace
 3. Any available counseling, rehabilitation and employee assistance programs; and
 4. Penalties that may be imposed upon employees for drug abuse violations.
- C. Provide as required by Government Code Section 8355(a)(3) that every employee who works under this Contract:
 1. Will receive a copy of the company's drug-free policy statement; and
 2. Will agree to abide by the terms of the company's statement as a condition of employment under this Contract.

D. Failure to comply with these requirements may result in suspension of payments under Contract or termination of Contract or both, and Contractor may be ineligible for award of any future County contracts if County determines that any of the following has occurred:

1. Contractor has made false certification, or
2. Contractor violates the certification by failing to carry out the requirements as noted above.

31. **EDD Independent Contractor Reporting Requirements:** Effective January 1, 2001, County of Orange is required to file in accordance with subdivision (a) of Section 6041A of the Internal Revenue Code for services received from a “service provider” to whom County pays \$600 or more or with whom County enters into a contract for \$600 or more within a single calendar year. The purpose of this reporting requirement is to increase child support collection by helping to locate parents who are delinquent in their child support obligations.

The term “service provider” is defined in California Unemployment Insurance Code Section 1088.8, subparagraph B.2 as “an individual who is not an employee of the service recipient for California purposes and who received compensation or executes a contract for services performed for that service recipient within or without the state.” The term is further defined by the California Employment Development Department to refer specifically to independent Contractors. An independent Contractor is defined as “an individual who is not an employee of the ... government entity for California purposes and who receives compensation or executes a contract for services performed for that ... government entity either in or outside of California.”

The reporting requirement does not apply to corporations, general partnerships, limited liability partnerships, and limited liability companies.

Additional information on this reporting requirement can be found at the California Employment Development Department website located at http://www.edd.ca.gov/Employer_Services.htm

The failure of Contractor to timely submit the requested data shall constitute a material breach and grounds for termination of this Contract.

32. **Emergency/Declared Disaster Requirements:** In the event of an emergency or if Orange County is declared a disaster area by County, state or federal government, Contract may be subjected to unusual usage. Contractor shall service County during such an emergency or declared disaster under the same terms and conditions that apply during non-emergency/disaster conditions. The pricing quoted by Contractor shall apply to serving County’s needs regardless of the circumstances. If Contractor is unable to supply the goods/services under the terms of Contract, then Contractor shall provide proof of such disruption and a copy of the invoice for the goods/services from Contractor’s supplier(s). Additional profit margin as a result of supplying goods/services during an emergency or a declared disaster shall not be permitted. In the event of an emergency or declared disaster, emergency purchase order numbers will be assigned. All applicable invoices from Contractor shall show both the emergency purchase order number and Contract number.

33. **Error and Omissions:** All reports, files and other documents prepared and submitted by Contractor shall be complete and shall be carefully checked by the professional(s) identified by Contractor as Project Manager and key personnel attached hereto, prior to submission to the County. Contractor agrees that County review is discretionary, and Contractor shall not assume that the County will discover errors and/or omissions. If the County discovers any errors or omissions prior to approving Contractor’s reports, files and other written documents, the reports, files or documents will be returned

to Contractor for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by the Contractor after County approval thereof, County approval of Contractor's reports, files or documents shall not be used as a defense by Contractor in any action between the County and Contractor, and the reports, files or documents will be returned to Contractor for correction.

34. **Equal Employment Opportunity:** Contractor shall comply with U.S. Executive Order 11246 entitled, "Equal Employment Opportunity" as amended by Executive Order 11375 and as supplemented in Department of Labor regulations (41 CFR, Part 60) and applicable state of California regulations as may now exist or be amended in the future. Contractor shall not discriminate against any employee or applicant for employment on the basis of race, color, national origin, ancestry, religion, sex, marital status, political affiliation or physical or mental condition.

Regarding handicapped persons, Contractor will not discriminate against any employee or applicant for employment because of physical or mental handicap in regard to any position for which the employee or applicant for employment is qualified. Contractor agrees to provide equal opportunity to handicapped persons in employment or in advancement in employment or otherwise treat qualified handicapped individuals without discrimination based upon their physical or mental handicaps in all employment practices such as the following: employment, upgrading, promotions, transfers, recruitments, advertising, layoffs, terminations, rate of pay or other forms of compensation, and selection for training, including apprenticeship. Contractor agrees to comply with the provisions of Sections 503 and 504 of the Rehabilitation Act of 1973, as amended, pertaining to prohibition of discrimination against qualified handicapped persons in all programs and/or activities as detailed in regulations signed by the Secretary of the Department of Health and Human Services effective June 3, 1977, and found in the Federal Register, Volume 42, No. 68 dated May 4, 1977, as may now exist or be amended in the future.

Regarding Americans with disabilities, Contractor agrees to comply with applicable provisions of Title 1 of the Americans with Disabilities Act enacted in 1990 as may now exist or be amended in the future.

35. **Equipment – Acceptance Testing:** Acceptance testing is intended to ensure that the equipment acquired operates in substantial accord with the Contractor's technical specifications, is adequate to perform as warranted by the Contractor, and evidences a satisfactory level of performance reliability prior to its acceptance by the County. If the equipment to be installed includes operating software as listed in the Contract or order, such operating software shall be present for the acceptance test unless substitute operating software acceptable to the County is provided. Acceptance testing may be required as specified in the Contract or order for all newly installed technology systems, subsystems, and individual equipment, and machines which are added or field modified, i.e. modification of a machine from one model to another, after a successful performance period.
36. **Equipment – Title to:** Unless otherwise specified in the Contract, order, or finance plan, title to the equipment shall remain with the Contractor and assigns, if any, until such time as the full purchase prices, applicable taxes, and interest charges, if any, are paid to the Contractor. Title to each machine will be transferred to the County when its purchase price, taxes, and associated interest charges, if any, are paid. Title to a special feature installed on a machine and for which only a single installation charge was paid shall pass to the County at no additional charge, together with title to the machine on which it was installed.
37. **Hazardous Conditions:** Whenever the Contractor's operations create a condition hazardous to traffic or to the public, the Contractor shall provide flagmen and furnish, erect and maintain control devices as are necessary to prevent accidents or damage or injury to the public at Contractor's expense and

without cost to the County. The Contractor shall comply with County directives regarding potential hazards.

Emergency lights and traffic cones must also be readily available at all times and must be used in any hazardous condition. Emergency traffic cones must be placed in front of and behind vehicles to warn oncoming traffic.

Signs, lights, flags, and other warning and safety devices shall conform to the requirements set forth in Chapter 6 of the current traffic manual, Traffic Control for Construction and Maintenance Work Zones, published by the State of California Department of Transportation.

38. **Headings:** The various headings and numbers herein, the grouping of provisions of this Contract into separate clauses and articles, and the organization hereof are for the purpose of convenience only and shall not limit or otherwise affect the meaning hereof.
39. **Inventions:** If any discover or invention arises or is developed in the course of, or as a result of work performed under this Contract, the Contractor shall refer to the discovery or invention to the County.
40. **Inventory:** County has an ongoing requirement for the commodities indicated in this Contract. Contractor shall maintain a reasonable stock on hand of all commodities for delivery upon request.
41. **Liquidated Damages:** It is agreed by and between the Contractor and the County that if this Contract is not fully and completely performed within the terms of the Contract, damage will be sustained by the County. Said damage includes any additional costs resulting from a delay in scheduled time frames by the Contractor. Since it is and will be impractical and extremely difficult to determine the actual damage which the County will sustain by reason of such delay, Contractor agrees to forfeit and pay to County the sum of \$20,000 (“Liquidated Damages”) for each calendar day that completion of all the work required by the Contract is delayed. County may deduct such sum from any payments due or to become due to Contractor. If the Liquidated Damages exceed the unpaid balance of the Contract price otherwise owed to Contractor, then Contractor shall immediately pay County the difference
42. **Mandatory Kick-Off Meeting:** Upon award of the contract, the awarded vendor(s) may be required to attend a mandatory kick-off meeting with County representatives to discuss important information related to the scope of work, the contract, and the invoice payment process. A quarterly check-in meeting may be required to review any issues with the contract.
43. **Material, Workmanship, and Acceptance:** All Materials furnished by Contractor in the work shall be new, high-grade, and free from defects. Quality of work shall be in accord with the general accepted standards. Materials, parts, equipment, and work quality shall be subject to County’s approval. Materials and work quality not conforming to the requirement of the Scope of Work shall be considered defective and shall be subject to rejection. Defective work or material, whether in place or not, shall be removed immediately from the site by Contractor, at its expense, when so directed by County.

If Contractor fails to replace any defective or damaged work or material within 48 hours after notice, County may cause such work or materials to be replaced. Replacement expense shall be deducted from the amount to be paid to Contractor.

Where materials are specified by reference to standard specifications of the American Society for Testing Materials (ASTM), American National Standards Institute (ANSI), Builders Hardware Manufacturers Association (BHMA), Federal Specifications, or others, all applicable provisions of the

designated specifications shall be considered as forming a part of the Contract documents to the same force and effect as if repeated therein.

44. **News/Information Release:** Contractor agrees that it will not issue any news releases in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval of said news releases from County through County's Project Manager.
45. **Notices:** Any and all notices, requests demands and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing with a copy provided to the assigned DPA, except through the course of the Parties' Project Managers' routine exchange of information and cooperation during the terms of the work and services. Any written communications shall be deemed to have been duly given upon actual in-person delivery, if delivery is by direct hand, or upon delivery on the actual day of receipt or no greater than four (4) calendar days after being mailed by US certified or registered mail, return receipt requested, postage prepaid, whichever occurs first. The date of mailing shall count as the first day. All communications shall be addressed to the appropriate party at the address stated herein or such other address as the Parties hereto may designate by written notice from time to time in the manner aforesaid.

Contractor:	TBD
Attn:	TBD
Address:	TBD
Phone:	TBD
Email:	TBD

County's Project Manager: John Wayne Airport/Planning & Development	
Attn:	TBD
Address:	3160 Airway Avenue Costa Mesa, CA 92626
Phone:	TBD
Email:	TBD

County's Project Manager: John Wayne Airport/Information Technology	
Attn:	TBD

Address:	3160 Airway Avenue Costa Mesa, CA 92626
Phone:	TBD
Email:	TBD
cc: John Wayne Airport/Procurement Services	
Attn:	TBD, County DPA
Address:	3160 Airway Avenue Costa Mesa, CA 92626
Phone:	TBD
Email:	TBD

46. **Order Dates:** Orders may be placed during the term of Contract even if delivery may not be made until after the term of Contract. Order dates take precedence over delivery dates. Contract must clearly identify the order date on all invoices to County.
47. **Payment Card Industry Data Security Standard (PCI DSS):** Contractor covenants and warrants that it is currently PCI DSS compliant and will remain compliant during the entire duration of this Contract. Contractor agrees to immediately notify County in the event Contractor should ever become non-compliant and will take all necessary steps to return to compliance and shall be compliant within ten (10) days of the commencement of any such interruption.
48. **Permits and Licenses:** Contractor shall be required to obtain any and all approvals, permits and/or licenses which may be required in connection with the permitted operation as set out herein. No permit approval or consent given hereunder by County in its governmental capacity shall affect or limit Contractor's obligations hereunder, nor shall any approvals or consents given by County as a party to this Contract, be deemed approval as to compliance or conformance with applicable governmental codes, laws, ordinances, rules, or regulations.
49. **Prevailing Wage:**
- A. **Prevailing Wage (Labor Code §1773):** Pursuant to the provisions of Section 1773 et seq. of the California Labor Code, Contractor shall comply with the general prevailing rates of per diem wages and the general prevailing rates for holiday and overtime wages in this locality for each craft, classification, or type of worker needed to execute Contract. The rates are available from the Director of the Department of Industrial Relations at the following website: <http://www.dir.ca.gov/dlsr/DPreWageDetermination.htm>. Contractor shall post a copy of such wage rates at the job site and shall pay the adopted prevailing wage rates. Contractor shall comply with the provisions of Sections 1775 and 1813 of the Labor Code.

- B. Labor Code Requirements:** Contractor and all Subcontractors shall comply with all applicable requirements of the Labor Code throughout the performance of Contract, including but not limited to the following:
- C. Labor Code Notice:** Contractor and all Subcontractors must comply with the requirements of Labor Code Section 1771.1(a), pertaining to registration of contractors pursuant to Section 1725.5. Bids cannot be accepted from unregistered contractors except as provided in Section 1771.1. This Project is subject to compliance monitoring and enforcement by the Department of Industrial Relations. After award of the Contract, Contractor and each Subcontractor shall furnish electronic payroll records directly to the Labor Commissioner in the manner specified in Labor Code Section 1771.4.
- D. Threshold Requirements for Prevailing Wages:** Except for public works projects of one thousand dollars (\$1,000) or less, not less than the general prevailing rate of per diem wages for work of a similar character in the locality in which the public work is performed, and not less than the general prevailing rate of per diem wages for holiday and overtime work fixed as provided in this chapter, shall be paid to all workers employed on public works.
- E. Wage Rates:** Contractor shall post a copy of the wage rates at the job site and shall pay the adopted prevailing wage rates as a minimum. Pursuant to the provisions of Section 1773 of the Labor Code of the State of California, the Board of Supervisors has obtained the general prevailing rate of per diem wages and the general prevailing rate for holiday and overtime work in this locality for each craft, classification, or type of workman needed to execute this Contract from the Director of the Department of Industrial Relations. These rates are on file with the Clerk of the Board of Supervisors. Copies may be obtained at cost at the office of County's OC Public Works/OC Facilities & Asset Management/A&E Project Management or visit the website of the Department of Industrial Relations, Prevailing Wage Unit at www.dir.ca.gov/DLSR/PWD. The Contractor shall comply with the provisions of Sections 1774, 1775, 1776 and 1813 of the Labor Code.
- F. Apprenticeship Requirements:** The Contractor shall comply with Section 230.1(A), California Code of Regulations as required by the Department of Industrial Relations, Division of Apprenticeship Standards by submitting DAS Form to the Joint Apprenticeship Committee of the craft or trade in the area of the site.
- G. Registration of Contractor:** All contractors and subcontractors must comply with the requirements of Labor Code Section 1771.1(a), pertaining to registration of contractors pursuant to Section 1725.5. Bids cannot be accepted from unregistered contractors except as provided in Section 1771.1. This project is subject to compliance monitoring and enforcement by the Department of Industrial Relations. After award of the contract, Contractor and each Subcontractor shall furnish electronic payroll records directly to the Labor Commissioner in the manner specified in Labor Code Section 1771.4.
- H. Prevailing Wage and DIR Requirement:** Awarding agencies are not required to submit the notice of contract award through DIR's PWC-100 system on projects that fall within the small project exemption. The small project exemption applies for all public works projects that do not exceed:
- \$25,000 for new construction, alteration, installation, demolition or repair
 - \$15,000 for maintenance
- If the project meets or exceeds these amounts, the County and the Contractor are required to register the project with the California Department of Industrial Relations.
- I. Payroll Records:** Contractor and any Subcontractor(s) shall comply with the requirements of Labor Code Section 1776. Such compliance includes the obligation to furnish the records specified

in Section 1776 directly to the Labor Commissioner in an electronic format, or other format as specified by the Commissioner, in the manner provided by Labor Code Section 1771.4. The requirements of Labor Code Section 1776 provide, in summary:

1. Contractor and any Subcontractor(s) performing any portion of the work under this Contract shall keep an accurate record, showing the name, address, social security number, work classification, straight time and overtime hours worked each day and week, and the actual per diem wages paid to each journeyman, apprentice, worker, or other employee employed by Contractor or any Subcontractor(s) in connection with the work.
 2. Each payroll record shall contain or be verified by a written declaration that it is made under penalty of perjury, stating both of the following:
 - a. The information contained in the payroll record is true and correct.
 - b. The employer has complied with the requirements of Labor Code Sections 1771, 1811, and 1815 for any work performed by his or her employees in connection with the Contract.
 3. The payroll records shall be certified and shall be available for inspection at the principal office of Contractor on the basis set forth in Labor Code Section 1776.
 4. Contractor shall inform County of the location of the payroll records, including the street address, city and county, and shall, within five (5) working days, provide a notice of any change of location and address of the records.
 5. Pursuant to Labor Code Section 1776, Contractor and any Subcontractor(s) shall have ten (10) days in which to provide a certified copy of the payroll records subsequent to receipt of a written notice requesting the records described herein. In the event that Contractor or any Subcontractor fails to comply within the ten (10) day period, he or she shall, as a penalty to County, forfeit one hundred dollars (\$100), or a higher amount as provided by Section 1776, for each calendar day, or portion thereof, for each worker to whom the noncompliance pertains, until strict compliance is effectuated. Contractor acknowledges that, without limitation as to other remedies of enforcement available to County, upon the request of the Division of Apprenticeship Standards or the Division of Labor Standards Enforcement of the California Department of Industrial Relations, such penalties shall be withheld from progress payments then due Contractor. Contractor is not subject to a penalty assessment pursuant to this section due to the failure of a subcontractor to comply with this section.
 6. Contractor and any Subcontractor(s) shall comply with the provisions of Labor Code Sections 1771 et seq., and shall pay workers employed on the Contract not less than the general prevailing rates of per diem wages and holiday and overtime wages as determined by the Director of Industrial Relations. Contractor shall post a copy of these wage rates at the job site for each craft, classification, or type of worker needed in the performance of this Contract, as well as any additional job site notices required by Labor Code Section 1771.4(b). Copies of these rates are on file at the principal office of County's representative, or may be obtained from the State Office, Department of Industrial Relations ("DIR") or from the DIR's website at www.dir.ca.gov. If the Contract is federally funded, Contractor and any Subcontractor(s) shall not pay less than the higher of these rates or the rates determined by the United States Department of Labor.
- J. **Work Hour Penalty:** Eight (8) hours of labor constitute a legal day's work, and forty hours constitute a legal week's work. Pursuant to Section 1813 of the Labor Code of the State of California, the Contractor shall forfeit to the County Twenty Five Dollars (\$25) for each worker employed in the execution of this Contract by the Contractor or by any subcontractor for each

calendar day during which such worker is required or permitted to work more than the legal day's or week's work, except that work performed by employees of said Contractor and subcontractors in excess of the legal limit shall be permitted without the foregoing penalty upon the payment of compensation to the workers for all hours worked in excess of eight (8) hours per day of not less than 1-1/2 times the basic rate of pay.

K. Wage Rate Penalty: Contractor and any Subcontractor(s) shall comply with the provisions of Labor Code Section 1775. Contractor and any Subcontractor(s) shall be subject to a penalty in an amount up to \$200, or a higher amount as provided by Section 1775, for each calendar day, or portion thereof, for each worker paid less than the prevailing wage rates for any work done by Contractor or Subcontractor(s) under Contract.

L. Apprentices: The Contractor acknowledges and agrees that, if this Contract involves a dollar amount greater than or a number of working days greater than that specified in Labor Code Section 1777.5, this Contract is governed by the provisions of Labor Code Section 1777.5. It shall be the responsibility of the Contractor to ensure compliance with this Article and with Labor Code Section 1777.5 for all apprenticeable occupations. Pursuant to Labor Code Section 1777.5 if that Section applies to this Contract as indicated above, the Contractor and any subcontractors under him employing workers in any apprenticeable craft or trade in performing any work under this Contract shall apply to the applicable joint apprenticeship committee for a certificate approving the Contractor or subcontractor under the applicable apprenticeship standards and fixing the ratio of apprentices to journeymen employed in performing the work. Pursuant to Labor Code Section 1777.5 if that Section applies to this Contract as indicated above, the Contractor and any subcontractor under him may be required to make contributions to the apprenticeship program. The Contractor and all subcontractors under him shall comply with Labor Code Section 1777.6 which Section forbids certain discriminatory practices in the employment of apprentices.

50. Precedence: Contract documents consist of this Contract and its exhibits and attachments. In the event of a conflict between or among Contract documents, the order of precedence shall be the provisions of the main body of this Contract, i.e., those provisions set forth in the recitals and articles of this Contract, and then the exhibits and attachments.

51. Project Manager, County: The County shall appoint a Project Manager to act as liaison between the County and the Contractor during the term of this Contract. The County's Project Manager shall coordinate the activities of the County staff assigned to work with the Contractor.

The County's Project Manager shall have the right to require the removal and replacement of the Contractor's Project Manager and key personnel. The County's Project Manager shall notify the Contractor in writing of such action. The Contractor shall accomplish the removal within three (3) business days after written notice from the County's Project Manager. The County's Project Manager shall review and approve the appointment of the replacement for the Contractor's Project Manager and key personnel. Said approval shall not be unreasonably withheld. The County is not required to provide any additional information, reason or rationale in the event it requires the removal of Contractor's Project Manager from providing further services under the Contract.

52. Protection of Restoration of Existing Areas: Contractor shall be responsible for protection of public and private property adjacent to the work. Contractor shall repair or replace all existing improvements that are damaged or removed as a result of their operation. Repairs and replacements shall be at least equal to existing improvements and shall match them in finish and dimension. All repairs shall be completed within two (2) working days from the damage notification unless otherwise approved by County Project Manager.

53. **Safety Data Sheets (SDS):** The Contractor is required to provide a completed Safety Data Sheet (SDS) for each hazardous substance provided to the County under the Contractor's Contract with the County. This includes hazardous substances that are not directly included in the Contract, but are included in the goods or services provided by the Contractor to the County. The provision of the SDSs must be in accordance with the requirements of California Labor Code Sections 6380 through 6399, General Industry Safety Order Section 5194, and Title 8, California Code of Regulations. The SDSs for each substance must be sent to the place of shipment or provision of goods/service.
54. **Subcontracting:** No performance of this Contract or any portion thereof may be subcontracted or otherwise delegated by Contractor, in whole or in part, without first obtaining the prior express written consent of County. Any attempt by Contractor to subcontract or delegate any performance of this Contract without the prior express written consent of County shall be invalid and shall constitute a material breach of this Contract, and any attempted assignment or delegation in derogation of this paragraph shall be void.
- In the event that Contractor is authorized by County to subcontract, this Contract shall take precedence over the terms of the agreement between Contractor and subcontractor, and any agreement between Contractor and a subcontractor shall incorporate by reference the terms of this Contract. Contractor shall remain responsible for the performance of this Contract and indemnification of County notwithstanding the County's consent to Contractor's request for approval of a subcontractor. Under no circumstances shall County be required to directly monitor the performance of any subcontractor. All work performed by a subcontractor must be monitored by Contractor and must meet the approval of the County of Orange pursuant to the terms of this Contract.
55. **Substitutions:** The Contractor is required to meet all specifications and requirements contained herein. No substitutions will be accepted without prior County written approval.
56. **Termination – Orderly:** After receipt of a termination notice from County of Orange, Contractor may submit to County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than 60 days from the effective date of the termination, unless one or more extensions in writing are granted by County upon written request of Contractor. Upon termination County agrees to pay Contractor for all services performed prior to termination which meet the requirements of Contract, provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in Contract. Upon termination or other expiration of this Contract, each party shall promptly return to the other party all papers, materials, and other properties of the other held by each for purposes of performance of Contract.
57. **Usage:** No guarantee is given by County to Contractor regarding usage of this Contract. Usage figures, if provided, are approximations. Contractor agrees to supply services and/or commodities requested, as needed by County of Orange, at rates/prices listed in Contract, regardless of quantity requested.
58. **Usage Reports:** Contractor shall submit usage reports on an annual basis to the assigned Deputy Procurement Agent of County of Orange user agency/department. The usage report shall be in a format specified by the user agency/department and shall be submitted 90 days prior to the expiration date of Contract term, or any subsequent renewal term, if applicable.
59. **Waivers – Contract:** The failure of the County in any one or more instances to insist upon strict performance of any of the terms of this Contract or to exercise any option contained herein shall not be construed as a waiver or relinquishment to any extent of the right to assert or rely upon any such terms or option on any future occasion.

Additional Terms and Conditions - Information Technology

1. **Software License:** Unless otherwise specified in the Scope of Work, the Contractor hereby grants to the County and the County accepts from the Contractor, subject to the terms and conditions of this Contract, an irrevocable, royalty-free, non-exclusive, license to use all Software of any type provided by Contractor to County.
2. **Future Releases:** Unless otherwise specifically provided in this Contract, or the Scope of Work, if improved versions, e.g., patches, bug fixes, Updates or releases, of any solution are developed by the Contractor, and are made available to other licensees, they will be made available to the County at no additional cost only if such are made available to other licensees at no additional cost. If the Contractor offers new versions or Upgrades to the solution, they shall be made available to the County at the County's option at a price no greater than the Contract price plus a price increase proportionate to the increase from the list price of the original version to that of the new version, if any. If the Software product has no list price, such price increase will be proportionate to the increase in average price from the original to the new version, if any, as estimated by the Contractor in good faith.
3. **Software Maintenance:** The correction of any residual errors in any software products which may be discovered by the Contractor or by the County will be considered maintenance. Such maintenance will be performed by the contractor without additional charge for the duration of this Contract. The contractor will be available to assist the County in isolating and correcting error conditions caused by the County's particular hardware or operating system at rates specified in this contract. If the contractor is called upon by the state to correct an error caused by the County's negligence, modification by the County, County-supplied data, or machine or operator failure or due to any other cause not inherent in the original software products, the contractor reserves the right to charge the County for such service on a time and material basis at rates in accordance with the contract.
4. **County Data:** Subject to applicable law, the County shall permit the Contractor and its subcontractors to have access to, and make appropriate use of, the information or material that the County submits to the Contractor pursuant to this Contract ("County Data"), solely to the extent the Contractor requires such access and use in order to properly and appropriately perform the Services as contemplated by this Contract. The Contractor may only access and use County Data in connection with performance of its duties under this Contract or as specifically directed by the County in writing and may not otherwise use, disclose, modify, merge with other data, commercially exploit, or make any other use of County Data or take, or refrain from taking, any other action that might, in any manner or form, adversely affect or jeopardize the integrity, security, or confidentiality of County Data, except as expressly permitted herein or as expressly directed by the County in writing. The Contractor acknowledges and agrees that, as between the Parties, the County owns all right, title, and interest in, and all Intellectual Property Rights in and to, all County Data.
5. **Acceptance Testing:** All Deliverables shall be provided to the County by the Contractor in conformity with all requirements, specifications, Acceptance Criteria, and time periods set forth or referenced in this Contract. The Contractor shall at all times utilize complete and thorough Acceptance Testing Procedures, and appropriate Acceptance Criteria, all of which shall be subject to review and approval in mutual agreement by the County's Project Manager and Contractor's Project Owner, and no such activities shall be deemed completed until all Acceptance Criteria, whether set forth in this Contract or mutually agreed upon by the Parties in writing, have been successfully met. Moreover, nothing in this section shall limit in any way the County's right to terminate immediately for cause pursuant to Paragraph K, Termination, herein.

- A. Acceptance Testing: Following the Contractor's notification to the County that the Contractor has completed any component or Deliverable identified in this Contract, at a mutually agreed scheduled time thereafter, the County shall begin testing the component or Deliverable to determine whether such component or Deliverable conforms to the applicable specifications and/or standards (collectively, the "Acceptance Criteria"). After the County has completed such testing or upon expiration of the agreed-upon testing period or any agreed-upon extension of the testing period (the "Acceptance Testing Period"), the County shall notify the Contractor in writing either that the component or Deliverable: (a) meets the Acceptance Criteria and that acceptance of such component or Deliverable has occurred ("Acceptance"); or (b) does not meet the Acceptance Criteria and the reasons therefor. If the component or Deliverable is identified as being part of a larger, integrated system being developed thereunder, then any Acceptance under the terms of this subsection shall be understood as being conditional acceptance ("Conditional Acceptance"), and such component or Deliverable shall be subject to Final Acceptance, as described below.
- B. Cure: If the County determines that a component or Deliverable does not conform to the applicable Acceptance Criteria, and that it is in the County's interest to allow the Contractor time to correct the problem, the County shall deliver to the Contractor a written exception report describing the nonconformity (the "Exception Report"). Within ten (10) calendar days following receipt of the Exception Report, the Contractor shall: (a) perform a Root Cause Analysis to identify the cause of the nonconformity; (b) provide the County with a written report detailing the cause of, and procedure for correcting, such nonconformity; (c) provide the County with satisfactory evidence that such nonconformity will not recur; and (d) use best efforts to correct critical errors (as determined by the County) and use commercially reasonable efforts to correct all other errors reasonably requested by the County and accepted by the Contractor; provided, however, that if the nonconformity of critical errors is incapable of cure within such ten (10) calendar day period then, within such ten (10) calendar day period, the Contractor shall present to the County a mutually agreeable plan to cure such nonconformity within a reasonable amount of time. Upon the Contractor's notice to the County that the Contractor has cured any such nonconformity, the County shall re-test the defective component or Deliverable for an additional testing period of up to thirty (30) calendar days or such other period as the Parties may mutually agree upon in writing, at the end of which period the process described in subsections (a) through (c) above shall be repeated. In the event the County rejects the component or Deliverable a second time and the Contractor disagrees with such rejection, then the Parties shall escalate the issue(s) to senior management of both Parties for mutual resolution.
- C. Final Acceptance: Upon achievement of Conditional Acceptance for all identified components or Deliverables, the County shall begin testing the System that is comprised of such components or Deliverables using the applicable test procedures and standards to determine whether such System performs as an integrated whole in accordance with the Acceptance Criteria. After the County has completed such testing or upon expiration of the testing period (the "Final Acceptance Testing Period"), the County shall notify the Contractor in writing that the System, and all components and Deliverables that are a part thereof: (a) meet the Acceptance Criteria and that final acceptance of the System and such components and Deliverables has occurred ("Final Acceptance"); or (b) does not meet the Acceptance Criteria and the reasons therefor. If the County determines that the Acceptance Criteria have not been so met, the process described in subsection (b) above shall be initiated, with all references to "component or Deliverable" being references to the "System," and all references to the "Acceptance Testing Period" being references to the "Final Acceptance Testing Period." Neither Conditional Acceptance, Acceptance nor Final Acceptance by the County shall constitute a waiver by the County of any right to assert claims based upon defects not discernible through conduct of the applicable test procedures and subsequently discovered in a component or Deliverable or the System following the County's Final Acceptance thereof. Nothing else,

including the County's use of the System, or any component thereof, shall constitute Final Acceptance, affect any rights and remedies that may be available to the County and/or constitute or result in "acceptance" under general contract law, any state uniform commercial code or any other law.

6. **Service Level Commitment:** Except as otherwise specified in this Contract, from and after the Effective Date, the Contractor shall perform the Services at levels that are equal to or better than the Service Level Requirements ("SLR") applicable to such Services. The Contractor shall be responsible for meeting or exceeding the applicable SLRs even where doing so is dependent on the provision of Services by subcontractors or other non-contractor personnel. The Service Level methodology applicable to the SLRs is set forth in Attachment D - JWA SLR Requirements. Any resources utilized by the Contractor pursuant to the terms hereof shall incorporate methods permitting measurement of all performance-related SLRs. The Contractor shall measure and compare the actual or observed performance resulting from the Contractor's performance of the Services with the SLRs during each month.
7. **Compatibility of Resources:** The Contractor shall ensure that the solution Software, all Services, and all Software, assets, Hardware, Equipment, and other resources and materials (collectively, the "Contractor Resources") that are provided by the Contractor to the County, otherwise utilized by the Contractor, or approved by the Contractor for utilization by the County, in connection with the use or operation of the solution, or with the providing or receiving of the Services, shall be successfully and fully integrated and interfaced, and shall be compatible, with, all applicable County Software, Services, Systems, items, and other resources (collectively, the "County Resources") that are owned by or leased or licensed to the County, or that are provided to the County by third party service providers. To the extent that any interfaces need to be developed or modified in order for the Contractor Resources to integrate fully and successfully and be compatible with the County Resources, the Contractor shall be responsible for the development or modification of such interfaces and for such integration, and all such activities shall be deemed to be Services within the scope of this Contract.
8. **Service Level Fee Reductions:** Failure by the Contractor to meet the application performance and service level guarantees as stated in Attachment D - JWA SLR Requirements, shall result in Fee Reductions. The Parties agree that the Fee Reductions reflect the diminished value of the Services as a result of Contractor failure to provide the Services in accordance with Attachment D - JWA SLR Requirements and, accordingly do not constitute nor shall be construed or interpreted as penalties. Fee Reductions shall in no event be the sole and exclusive remedy of County with respect to any failure of the Contractor as described in this clause. Fee Reductions shall be in the based upon Attachment D - JWA SLR Requirements. The Contractor shall provide a corrective action plan in accordance with Attachment D - JWA SLR Requirements if identification of performance issues.
9. **Data Location:** Except where the Contractor obtains the County's prior written approval, the physical location of the Contractor's data center where County Data is stored shall be within the United States.
10. **Source Code and Contractor's Insolvency:** In the event Contractor becomes insolvent or bankrupt, Contractor shall grant to the County a nonexclusive, nontransferable license for access and use to Contractor's Agenda System Source Code and documentation for the use restricted by this contract. County agrees:
 - A. That no copies of the Source Code in any form will be given by the County to any third party except as expressly permitted under the terms of this Contract or required by law, except that access or use by the County or its subcontractors (if any) solely for the purposes of maintaining, upgrading, modifying, or enhancing the Agenda System Software shall be permitted;

- B. To reproduce Contractor's copyright notice on all material related to or part of the Contractor's Agenda System on which any such copyright notice is displayed, including any copies made pursuant to this Contract;
- C. Not to remove any copyright notices, trademark credits, confidentiality notice, mark, legend, or other information included in the Contractor's Agenda System; and
- D. Not to purport to sell, transfer, or assign any intellectual property rights or other rights in or to the Contractor's Agenda System except as expressly permitted by this Contract.

11. **Disentanglement Process:** In the event of expiration of the Term or termination of this Contract, in whole or in part, the Contractor shall perform disentanglement services to transition responsibility for the provision of Services to a replacement contractor or to the County itself ("Disentanglement Services"). The Disentanglement Services shall begin on the expiration date of the Term or termination date of this Contract and, unless the Parties subsequently agree in writing to extend the Term, the Contractor shall continue to provide Disentanglement Services, in accordance with Attachment E - Disentanglement List requirements or as the County reasonably requests, until the earlier of a Disentanglement satisfactory to the County has been completed or twelve (12) months after the expiration of the Term or termination date, as appropriate.

As soon as reasonably practicable after the Disentanglement Services begin, the Contractor and the County shall develop a plan in good faith that specifies the tasks to be performed by the Parties during disentanglement and the schedule for the performance of such tasks. Unless otherwise agreed by the Parties in writing, such plan shall not in any respect lessen or eliminate the Contractor's obligations under this Contract to provide all Disentanglement Services necessary and reasonably requested by the County. The plan will be developed, implemented, and concluded with full disentanglement with all due speed, not to exceed twelve (12) months.

The Parties shall cooperate fully with one another, and any replacement contractor, to facilitate a smooth transition of the Services from the Contractor to the replacement contractor or the County. The Disentanglement Services shall be provided to the County by the Contractor regardless of the reason for termination or expiration. The Contractor shall continue to provide the Services during disentanglement in a manner consistent with the Contractor's provision and performance of such Services during the period such Services were provided to the County hereunder, with no material interruption of the Services and no material adverse impact on the provision of the Services.

All Disentanglement Services performed by the Contractor shall be performed by the Contractor at no additional cost to the County beyond what the County would pay for the Services.

- 12. **Trans-Border Data Flows:** Contractor shall not transfer any County Data across a country border.
- 13. **Obsolete and Unsupported Software or Hardware:** Contractor shall notify County of any hardware or software currently in use that will go unsupported within nine (9) months of obsolescence. Contractor shall ensure that notice is sent to the County's Project Manager and JWA Procurement Services department with a report that details the support needed to maintain operational status and a proposal to maintain operational status beyond obsolescence.

Additional Terms and Conditions - Information Technology Security Guidelines

All contractors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines for all Controls one (1) thru six (6) below at all times during the term of its contract with County.

1. **Asset Management:**

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that shall allow the assets to maintain productivity during disruptive events. There are four broad categories of assets: people, information, technology, and facilities.

The Cybersecurity Program strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data.

A. **Goals and Objectives**

1. Services are identified and prioritized.
2. Assets are inventoried, and the authority and responsibility for these assets is established.
3. The relationship between assets and the services they support is established.
4. The asset inventory is managed.
5. Access to assets is managed.
6. Information assets are categorized and managed to ensure the sustainment and protection of the critical service.
7. Facility assets supporting the critical service are prioritized and managed.

B. **Asset Management Policy Statements**

1. **Services Inventory**

- a. Departments and/or contractors shall maintain an inventory of its services. This listing shall be used by the department to assist with its risk management analysis.

2. **Asset Inventory – Information**

- a. All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property shall be used in compliance with this policy.
- b. County information is a valuable asset and shall be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices shall be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.
- c. Departments and/or contractors shall establish internal procedures for the secure handling and storage of all electronically-maintained County information that is owned or controlled by the department.

3. **Asset Inventory - Technology (Devices, Software)**

- a. Departments shall maintain an inventory of all department managed devices that connect to County network resources or processes, stores, or transmits County data including but not limited to:

- i. Desktop computers,
 - ii. Laptop Computers,
 - iii. Tablets (iPads and Android devices),
 - iv. Mobile Phones (basic cell phones),
 - v. Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),
 - vi. Servers,
 - vii. Storage devices,
 - viii. Network switches,
 - ix. Routers,
 - x. Firewalls,
 - xi. Security Appliances,
 - xii. Internet of Things (IoT) devices,
 - xiii. Printers,
 - xiv. Scanners,
 - xv. Kiosks and Thin clients,
 - xvi. Mainframe Hardware, and
 - xvii. VoIP Phones.
- b. Asset inventory shall map assets to the services they support.
 - c. Departments and/or contractors shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased).
 - d. Each department and/or contractor shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.
- 4. Asset Inventory - Facilities**
- a. Departments and/or contractors shall maintain an inventory of its facilities. This listing shall be used by the department to assist with its risk management analysis.
 - b. Departments and/or contractors shall identify the facilities used by its critical services.
- 5. Access Controls**
- a. Departments and/or contractors shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.
 - b. Access to County information systems and information systems data shall be based on each user's access privileges. Access controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle.

- c. Access to County information and County information assets should be based on the principle of “least privilege,” that is, grant no user greater access privileges to the information or assets than County responsibilities demand.
 - d. The owner of each County system, or their designee, provides written authorization for all internal and external user access.
 - e. All access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier (ID) and password combination that provides verification of the user’s identity.
 - f. All County workforce members are to be assigned a unique user ID to access the network, as applicable.
 - g. A user account shall be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need shall be documented prior to account creation and accounts activated only when necessary.
 - h. User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.
 - i. Departments and/or contractors shall conduct regular reviews of the registered users’ access level privileges. System owners shall provide user listings to departments for confirmation of user’s access privileges.
- 6. Asset Sanitation/Disposal**
- a. Unless approved by County management, no County computer equipment shall be removed from the premises.
 - b. Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.
 - c. Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.
 - d. Sanitization methods for media containing County information shall be in accordance with NSA (National Security Agency) standards (for example, clearing, purging, or destroying).
 - e. Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

2. Controls Management:

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. This process helps the organization ensure the controls management objectives are satisfied.

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess.

A. Goals and Objectives

1. Control objectives are established.

2. Controls are implemented.
3. Control designs are analyzed to ensure they satisfy control objectives.
4. Internal control system is assessed to ensure control objectives are met.

B. Control Management Policy Statements

1. Physical and Environmental Security

- a. Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.
- b. Restricted areas within facilities that house sensitive or critical County information systems shall, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.
- c. Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.
- d. Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.
- e. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.
- f. Continuity of power shall be provided to maintain the availability of critical equipment and information systems.
- g. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Different, yet appropriate methods shall be utilized for internal and external cabling.
- h. Equipment shall be properly maintained to ensure its continued availability and integrity.
- i. All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.

2. Network Segmentation

NOTE: This section is applicable to Departments that manage their own network devices.

- a. Segment (e.g., VLANs) the network into multiple, separate zones (based on trust levels of the information stored/transmitted) to provide more granular control of system access and additional intranet boundary defenses. Whenever information flows over a network of lower trust level, the information shall be encrypted.
- b. Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.
- c. Create separate network segments (e.g., VLANs) for BYOD (bring your own device) systems or other untrusted devices.
- d. The network infrastructure shall be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3. **Mobile Computing Devices**

To ensure that Mobile Computing Devices (MCDs) do not introduce threats into systems that process or store County information, departments' and/or contractors' management shall:

- a. Establish and manage a process for authorizing, issuing and tracking the use of MCDs.
- b. Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.
- c. Implement applicable access control requirements in accordance with this guideline, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.
- d. Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information.
- e. Ensure that MCDs are configured to restrict the user from circumventing the authentication process.
- f. Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.
- g. Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.
- h. The installation of any software, executable, or other file to any County computing device is prohibited if that software, executable, or other file downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds unless approved by the department.

4. **Personally Owned Devices**

Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (PDA's) owned by or purchased by employees, contract personnel, or other non-County users.

- a. The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless previously approved.
- b. The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County's SaaS applications. Access to some agency specific applications, e.g. applications that are subject to compliance regulations may require prior approval of the County CISO and the associated Department Head.
- c. The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources.
- d. The County will only request access to the personally owned device in order to implement security controls; to respond to litigation hold (aka: e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized technician or designee using a legitimate software process.

5. Logon Banners and Warning Notices

- a. At the time of network login, the user shall be presented with a login banner.
- b. All computer systems that contain or access County information shall display warning banners informing potential users of conditions of use consistent with state and federal laws.
- c. Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.
- d. The banner message shall be placed at the user authentication point for every computer system that contains or accesses County information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.
- e. At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:
 - i. User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.
 - ii. System usage may be monitored, recorded, and subject to audit.
 - iii. Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
 - iv. Use of the system indicates consent to monitoring and recording.

6. Authentication

- a. Authenticate user identities at initial connection to County resources.
- b. Authentication mechanisms shall be appropriate to the sensitivity of the information contained.
- c. Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

7. Passwords

- a. County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices and personally owned devices used for work.
- b. Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:
 - i. Passwords will contain a minimum of one (1) upper case letter
 - ii. Passwords will contain a minimum of one (1) lower case letter
 - iii. Passwords will contain a minimum of one (1) number: 1- 0
 - iv. Passwords will contain a minimum of one (1) special character: !, @, #, \$, %, ^, &, *, (,)
 - v. Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
 - vi. Passwords characters will not be repeated in a row (Do not use: P@\$\$\$. This is ok: P@\$\$)

vii. COMPLEX PASSWORD EXAMPLE: P@\$SWoRd13

viii. Passphrases example: The\$kyIsBlue2day

ix. Passwords cannot contain the user's full name or network login.

- c. Passwords shall have a minimum length of twelve (12) characters.
- d. Passwords shall not be reused for twelve (12) iterations.
- e. Departments and/or contractors shall require users to change their passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.
- f. Network and application systems shall be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum) when the technology is feasible or available.
- g. Newly created accounts shall be assigned a randomly generated password prior to account information being provided to the user.
- h. No user shall give his or her password to another person under any circumstances. Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management.
- i. Users who have lost or forgotten their passwords shall make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester shall be authenticated to the user account in question. (e.g., Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords shall be provided directly and only to the user in question.
- j. When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.
- k. All passwords are to be treated as sensitive information.
- l. User Accounts shall be locked after five consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID after investigation. These features shall be configured as indicated when the technology is feasible or available.
- m. All systems containing sensitive information shall not allow users to have multiple concurrent sessions on the same system when the technology is feasible or available.

C. Inactivity Timeout and Restricted Connection Times

1. Automatic lockouts for system devices, including workstations and mobile computing devices, after no more than 15 minutes of inactivity.
2. Automated screen lockouts shall be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures shall be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members shall not leave their computer unattended or available for someone else to use.

3. When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections shall be accepted.

D. Account Monitoring

1. Access to a County network and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These shall be secured to ensure County resources are not accessed by unauthorized users.)
2. The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.
3. Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.
4. After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.
5. On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

E. Administrative Privileges

1. Systems Administrators shall use separate administrative accounts, which are different from their end user account (required to have an individual end user account), to conduct system administration tasks.
2. Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.
3. Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative using the Security Review and Approval Process.
4. Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the Security Review and Approval Process.
5. Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.
6. All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Controls Management B.7.

F. Remote Access

1. Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.
2. Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.

3. All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by the County. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.
4. Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.
5. All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.
6. All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.
7. Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.
8. Users granted remote access to County IT infrastructure shall follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.
9. Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.
10. All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department and the County. This approval shall be received prior to the start of such implementation.
11. Remote access privileges to County IT resources shall not be given to contractors and customers unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.

G. Wireless Access

1. Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.
2. Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.
3. County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.
4. All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, vendors and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.

5. Each department and/or contractor shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

H. System and Network Operations Management

1. Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.
2. Departments and/or contractors shall establish controls to ensure the security of the information systems networks that they operate.
3. Operational system documentation for County information systems shall be protected from unauthorized access.
4. System utilities shall be available to only those users who have a business case for accessing the specific utility.

I. System Monitoring and Logging

1. Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.
2. Each department and/or contractor shall maintain a log of all faults involving County information systems and services.
3. Logs shall be protected from unauthorized access or modifications wherever they reside.
4. The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.
5. Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.
6. Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

J. Malware Defenses

1. Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and white listing and black listing of applications, web sites, and IP addresses.
2. Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.
3. Where feasible, any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network shall be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

K. Data Loss Prevention

1. Departments and/or contractor shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.
2. Departments and/or contractors shall deploy encryption software on mobile devices containing sensitive.

L. Data Transfer

1. Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.
2. County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

M. Encryption

1. The decision to use cryptographic controls and/or data encryption in an application shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.
2. The decision to use cryptographic controls and/or data encryption on a hard drive shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.
3. Where appropriate, encryption shall be used to protect confidential application data that is transmitted over open, untrusted networks, such as the Internet.
4. When cryptographic controls are used, procedures addressing the following areas shall be established by each department:
 - a. Determination of the level of cryptographic controls
 - b. Key management/distribution steps and responsibilities
5. Encryption keys shall be exchanged only using secure methods of communication.

N. System Acquisition and Development

1. Departments and/or contractors shall identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the department as well as other business applications that are used by the department but owned and/or managed by other County organizations. All business applications used by a department shall be documented in the department's IT security plan as well as their Business Impact Analysis (BIA) for critical rating (RTO) and continuity purposes.
2. An application owner shall be designated for each internal department business application.
3. All access controls associated with business applications shall be commensurate with the highest level of data used within the application. These same access controls shall also adhere to the policy provided in Section 1.2.5: Access Controls.
4. Security requirements shall be incorporated into the evaluation process for all commercial software products that are intended to be used as the basis for a business application. The security requirements in question shall be based on requirements and standards specified in this guideline.
5. In situations where data needs to be isolated because there would be a conflict of interest, data security shall be designed and implemented to ensure that isolation.

O. Business Requirements

1. The business requirements definition phase of system development shall contain a review to ensure that the system shall adhere to County information security standards.

P. System Files

1. Operating system files, application software and data shall be secured from unauthorized use or access.
2. Clear-text data that results from testing shall be handled, stored, and disposed of in the same manner and using the same procedures as are used for production data.
3. System tests shall be performed on data that is constructed specifically for that purpose.
4. System testing shall not be performed on operational data unless the necessary safeguards are in place.
5. A combination of technical, procedural and physical safeguards shall be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

Q. System Development & Maintenance

1. The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.
2. When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade shall be completed in advance in order to minimize potential security risks and disruptions to the production environment.
3. Any outside suppliers used for maintenance that are visitors to the facility are to be escorted and monitored while performing maintenance to critical systems. This does not apply to contractors that are assigned to work at the facility.
4. Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.
5. All County workforce members, including contractors, shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.
6. In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.
7. Departments and/or contractors are responsible for managing outsourced software development related to department-owned IT systems.

R. System Requirements

1. Any system that processes or stores County Information shall:
 - a. Baseline configuration shall incorporate Principle of Least Privilege and Functionality.

- b. Systems shall be deployed where feasible to utilize existing County authentication methods.
- c. Session inactivity timeouts shall be implemented for all access into and from County networks.
- d. All applications are to have access controls unless specifically designated as a public access resource.
- e. Meet the password requirements defined in Section 2.2.7: Passwords.
- f. Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.
- g. Monitor special privilege access, e.g. administration accounts.
- h. Restrict authority to change master files to persons independent of the data processing function.
- i. Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.
- j. Be capable of routinely monitoring the access to automated systems containing County Information.
- k. Log all modifications to the system files.
- l. Limit access to system utility programs to necessary individuals with specific designation.
- m. Delete or disable all default accounts.
- n. Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes shall be applied only through the appropriate change control process.
- o. Restrict access to server-file-system controls that allow access to other users' files.
- p. Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

S. Procurement Controls

- 1. Breach notification requirements clause to be included in new or renewal contracts for systems containing sensitive information.
- 2. Contractor shall report to the County within 24 hours as defined in this contract when Contractor becomes aware of any suspected data breach of contractor's or subcontractor's systems involving County's data.
- 3. Departments shall review all procurements and renewals for software and equipment (hosted/managed by the vendor) that transmits, stores, or processes sensitive information to ensure that contractors are aware of and are in compliance with County's cybersecurity policies, if applicable. Departments shall obtain documentation supporting the business partners, contractors, or consultants' compliance with County's cybersecurity policies such as:
 - a. SOC 1 Type 2

- b. SOC 2 Type 2
- c. Security Certifications (ISO, PCI, etc.)
- d. FedRAMP certification
- e. Penetration Test Results

T. IT Services Provided to Public

1. Public access to County electronic information resources shall provide desired services in accordance with safeguards designed to protect County resources. All County electronic information resources are to be reviewed at least quarterly.

U. Removable Media

1. When no longer required, the contents of removable media shall be permanently destroyed or rendered unrecoverable in accordance with applicable department, County, state, or federal record disposal and/or retention requirement.

3. Configuration & Change Management:

Configuration and Change Management (“CCM”) is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

Cybersecurity is an integral component to information systems from the onset of the project or acquisition through implementation of:

- A. Application and system security
- B. Configuration management
- C. Change control procedures
- D. Encryption and key management
- E. Software maintenance, including but not limited to, upgrades, antivirus, patching and malware detection response systems

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization.

A. Goals and Objectives

1. The lifecycle of assets is managed.
2. The integrity of technology and information assets is managed.
3. Asset configuration baselines are established.

B. Configuration & Change Management Policy Statements

1. Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.
2. Changes impacting security appliances managed by OCIT (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by County in accordance with the County Security Review and Approval Process.
3. Only authorized users shall make any changes to system and/or software configuration files.
4. Only authorized users shall download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems without prior written authorization from department IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.
5. Each department and/or contractor shall develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.
6. Each department and/or contractor shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.
7. As appropriate, segregation of duties shall be implemented by all County departments to ensure that no single person has control of multiple critical systems and the potential for misusing that control.
8. Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.
9. System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
10. System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.

4. Vulnerability Management:

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

A. Goals and Objectives

1. Preparation for vulnerability analysis and resolution activities is conducted.
2. A process for identifying and analyzing vulnerabilities is established and maintained.
3. Exposure to identified vulnerabilities is managed.
4. The root causes of vulnerabilities are addressed.

B. Vulnerability Management Policy Statements

1. Departments and/or contractors shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.

5. Cybersecurity Incident Management:

Information Security Incident Management establishes the policy to be used by each department and/or contractor in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that:

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

This domain defines management controls for addressing cyber incidents. The controls provide a consistent and effective approach to Cyber Incident Response aligned with Orange County's Cyber Incident Response Plan, to include:

- Collection of evidence related to the cyber incident as appropriate
- Reporting procedures including any and all statutory reporting requirements
- Incident remediation
- Minimum logging procedures
- Annual testing of the plan

A. Goals and Objectives

1. A process for identifying, analyzing, responding to, and learning from incidents is established.
2. A process for detecting, reporting, triaging, and analyzing events is established.
3. Incidents are declared and analyzed.
4. A process for responding to and recovering from incidents is established.
5. Post-incident lessons learned are translated into improvement strategies.

B. Cybersecurity Incident Management Policy Statements

1. Cybersecurity incident management procedures shall be established within each department and/or contractor to ensure quick, orderly, and effective responses to security incidents. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan. The steps involved in managing a security incident are typically categorized into six stages:
 - a. System preparation
 - b. Problem identification
 - c. Problem containment
 - d. Problem eradication
 - e. Incident recovery

- f. Lessons learned
2. The department shall act as the liaison between applicable parties during a cybersecurity incident. The department shall be the primary point of contact for all IT security issues.
 3. A designated security contact for all cybersecurity incidents.
 4. Departments and/or contractors shall conduct periodic (at least annually) cybersecurity incident scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.
 5. Departments and/or contractors shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan.
 6. Each department and/or contractor shall familiarize its employees on the use of its cybersecurity incident reporting procedures.
 7. Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.
 8. Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.
 9. Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.
 10. Departments shall report cybersecurity incidents to the County pursuant to the Contract.

6. Service Continuity Management:

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission. Services that are most important to an organization's ability to meet its mission are considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services.

This domain defines requirements to document, implement and annually test plans, including the testing of all appropriate cybersecurity provisions, to minimize impact to systems or processes from the effects of major failures of information systems or disasters via adoption and annual testing of:

- Business Continuity Plan
- Disaster Recovery Plan
- Cyber Incident Response Plan

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

A. Goals And Objectives

1. Service continuity plans for high-value services are developed.
2. Service continuity plans are reviewed to resolve conflicts between plans.
3. Service continuity plans are tested to ensure they meet their stated objectives.
4. Service continuity plans are executed and reviewed.

B. Service Continuity Management Policy Statements

1. Backups of all essential electronically-maintained County business data shall be routinely created and properly stored to ensure prompt restoration.
2. Each department and/or contractor shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the department.
3. The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.
4. Departments and/or contractors shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.
5. Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.
6. Departments and/or contractors shall define and periodically test a formal procedure designed to verify the success of the backup process.
7. Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.
8. Departments and/or contractors shall retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.
9. Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.

10. Each department and/or contractor shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.
11. Departments and/or contractors shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). RAs include department identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the department has deemed critical after performing a risk analysis.
12. Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.
13. Each department and/or contractor shall maintain a comprehensive plan document containing its business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans shall be prepared in accordance with the standards established by the County's Business Continuity Management Policy.
14. Each department and/or contractor shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.

Additional Terms and Conditions - Information Technology Security Provisions

1. Contractor's Policies, Procedures, and Technical, Physical, and Administrative Safeguards:

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to:

- A. Ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services,
- B. Protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information,
- C. Protect against unauthorized access, use, or disclosure of personal or County confidential information,
- D. Maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches,
- E. Ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and
- F. Ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

2. County of Orange Information Technology Security Provisions Document:

This County of Orange Information Technology Security Provisions document provides a high-level guide for contractors to understand the resiliency and cybersecurity expectations of the County. The County of Orange Security Guidelines follow the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all County of Orange Information Technology Security Provisions ("Security Provisions") that pertain to Contractor(s) in connection with the Services performed by Contractor(s) as set forth in the scope of work of this Contract. Any violations of the Security Provisions shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Provisions include, but are not limited to, County of Orange Information Technology Security Guidelines, as applicable, and Business Associate Agreement.

Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this Contract.

3. Contractor's Information Security Program:

The Contractor shall implement and maintain a written information security program that contains reasonable and appropriate security measures designed to safeguard the confidentiality, integrity, availability, and resiliency of County data and/or system(s). The Contractor shall review and update its information security program in accordance with contractual, legal, and regulatory requirements. Contractor shall provide to County a copy of the organization's information security program and/or policies.

4. Information Access:

- A. Contractor shall use appropriate safeguards and security measures to ensure the confidentiality and security of all County data. County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.
- B. Throughout the Contract term, upon request from County but at least once each calendar year, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel and/or subcontractor personnel having access to County systems and/or County data, and the respective security level or clearance assigned to each such Contractor personnel and/or subcontractor personnel. County reserves the right to require the removal and replacement of Contractor personnel and/or subcontractor personnel at the County's sole discretion. Removal and replacement shall be performed within 14 calendar days of notification by the County.

- C. All County resources (including County systems), County data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed by such Contractor and/or subcontractors personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor or Contractor's personnel and subcontractors, at any time.
- D. Contractor acknowledges and agrees that any failure to comply with the provisions of this paragraph shall constitute a breach of this Contract and entitle County to deny or restrict the rights of such non-complying Contractor personnel and/or subcontractor personnel to access and use the County data and/or system(s), as County in its sole discretion shall deem appropriate.

5. Data Security Requirements:

- A. Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor must establish, maintain, and enforce a data privacy program and an information and cyber security program, including safety, physical, and technical security and resiliency policies and procedures, that comply with the requirements set forth in this Contract and, to the extent such programs are consistent with and not less protective than the requirements set forth in this Contract and are at least equal to applicable best industry practices and standards (NIST 800-53).
- B. Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data, Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject to civil and criminal sanctions contained in applicable federal and state statutes.
- C. Contractor shall take all reasonable measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against hackers and others who may seek, without authorization, to disrupt, damage, modify, access, or otherwise use Contractor systems or the information found therein; and prevent County data from being commingled with or contaminated by the data of other customers or their users of the Services and unauthorized access to any of County data.
- D. Contractor shall also continuously monitor its systems for potential areas where security could be breached. In no case shall the safeguards of Contractor's data privacy and information and cyber security program be less stringent than the safeguards used by County. Without limiting any other audit rights of County, County shall have the right to review Contractor's data privacy and information and cyber security program prior to commencement of Services and from time to time during the term of this Contract.
- E. All data belongs to the County and shall be destroyed or returned at the end of the contract via digital wiping, degaussing, or physical shredding as directed by County.

6. Enhanced Security Measures:

County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth, in reasonable detail, the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall cause Contractor personnel and subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

7. General Security Standards:

Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor (“Contractor Systems”) to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

- A. **Contractor System(s) and Security:** At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County’s access and use of County data and the Services.

- B. **Contractor and the use of Email:** Contractor, including Contractor’s employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor’s employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor’s performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County’s express prior written approval. Contractors who are not provided with a County email address, but need to transmit County data will be required to maintain and transmit County data in accordance with this Agreement.

8. Security Failures:

Any failure by the Contractor to meet the requirements of this Contract with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this Contract and may result in termination and reimbursement to County of any fees prepaid by County prorated to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the Contract.

9. **Security Breach Notification:**

- A. In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense,
1. Immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence;
 2. Perform a root cause analysis of the actual, potential, or suspected breach;
 3. Provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents;
 4. Conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and
 5. Cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and
 6. Perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).
- B. County shall make the final decision on notifying County officials, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Contractor shall reimburse County for all notification and related costs incurred by County arising out of or in connection with any such occurrence due to Contractor's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.
- C. In the case of a breach, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.
- D. Contractor shall indemnify, defend with counsel approved in writing by County, and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence.

Notification shall be sent to:

Andrew Alipanah, MBA, CISSP
 Chief Information Security Officer
 721 S. Parker St.
 Suite 200
 Orange, CA 92868

Phone: (714) 567-7611
Andrew.Alipanah@ocit.ocgov.com

Linda Le, CHPC, CHC, CHP
 County Privacy Officer
 721 S. Parker St.
 Suite 200
 Orange, CA 92868
 Phone: (714) 834-4082
Linda.Le@ocit.ocgov.com

10. **Security Audits:**

- A. Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup, disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures).
- B. Contractor shall inform County of any internal/external security audit or assessment performed on Contractor's operations, information and cyber security program, disaster recovery plan, and prevention, detection, or response protocols that are related to hosted County content, within sixty (60) calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within thirty (30) days after Contractor's receipt of request for such report(s).
- C. Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to penetration testing of any cloud-based solution provided by Contractor to County under this Contract. Contractor shall implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information/cyber security program.
- D. In addition, County has the right to review Plans of Actions and Milestones (POA&M) for any outstanding items identified by the SOC 2 Type II report requiring remediation as it pertains to the confidentiality, integrity, and availability of County data. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof without limitation and without liability to County if County reasonably determines Contractor fails or has failed to meet its obligations under this section

11. **Business Continuity and Disaster Recovery (BCDR):**

- A. For the purposes of this section, "Recovery Point Objectives" means the maximum age of files (data and system configurations) that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure (establishing the data backup schedule and strategy). "Recovery Time Objectives" means the maximum duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a loss of functionality.
- B. The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and operations of the County.

Business continuity management will enable the Contractor to identify and minimize disruptive risks and restore and recover hosted County business-critical services and/or data within the agreed terms following an adverse event or other major business disruptions. Recovery and timeframes may be impacted when events or disruptions are related to dependencies on third-parties. The County and Contractor will agree on Recovery Point Objectives and Recovery Time Objectives (as needed) and will periodically review these objectives. Any disruption to services of system will be communicated to the County within 4 hours, and every effort shall be undertaken to restore contracted services, data, operations, security, and functionality.

- C. All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

(signature page follows)

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract on the date following their respective signatures.

TBD/CONTRACTORS NAME*

If the Contractor is a corporation, signatures of two specific corporate officers are required as further set forth.

- The first corporate officer signature must be one of the following: 1) Chairman of the Board, 2) President, 3) Vice President; and
- The second corporate officer signature must be one of the following: 1) Secretary, 2) Assistant Secretary, 3) Chief Financial Officer, 4) Assistant Treasurer.

In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signature to bind the company.

Signature	Name	Title	Date
-----------	------	-------	------

Signature	Name	Title	Date
-----------	------	-------	------

COUNTY OF ORANGE, a political subdivision of the State of California
COUNTY AUTHORIZED SIGNATURE:

Signature	Name	Deputy Procurement Agent Title	Date
-----------	------	-----------------------------------	------

Approved as to form:
 County Counsel

Signature	Name	Deputy Title	Date
-----------	------	-----------------	------

ATTACHMENT A
SCOPE OF WORK

1. PURPOSE AND BACKGROUND

John Wayne Airport (JWA) is seeking proposals for Common Use Passenger Processing (CUPPS) and Common Use Self Service (CUSS) Systems Replacement & Support Services. The scope of work includes disposal of the existing CUPPS and CUSS systems, and the phased deployment of the new systems, in coordination with County and airline personnel training. The Contractor shall furnish all materials, equipment, labor, supervision and services necessary to install and implement fully operating CUPPS and CUSS systems as specified herein. This includes, but is not limited to, supply, delivery, unloading, setting, anchoring, electrical and data wiring installation and termination, new equipment, software, system integration, maintenance and support services. All installations done pursuant to this Contract shall be routine and usual work that is incidental to the replacement of the CUPPS/CUSS equipment. The full scope of this desired platform is detailed below. Contractor shall provide a turn-key solution that includes all professional services, materials/equipment, and site administration/maintenance offering that meet the County's requirements as defined in this section.

2. SCOPE OF WORK

The work in this section includes the disposal of all existing CUPPS and CUSS system equipment and furnishing all material, equipment, software, integration, labor, and supervision to install in place fully operating CUPPS and CUSS systems as specified herein. The scope of the project includes but is not limited to the design, development, all associated equipment and software, programming, integration with existing systems (e.g. Content Management System (CMS) and IED Globalcom Mass Notification System, Baggage Handling System), fabrication, packaging, shipping, delivery, unloading, setting/installation of all hardware and software, peripherals, and associated mounts, anchoring, electrical and data wiring installation, electrical and data wiring termination, start up, unit testing, reliability testing, systems testing, and on-site training of County staff and airline staff, and complete documentation of CUPPS and CUSS systems. All installations done pursuant to this contract shall be routine and usual work that is incidental to the replacement of the CUPPS/CUSS equipment. The system shall support multiple credentials for access control and payment services and shall comply with the most current Payment Card Industry (PCI) Data Security Standards (DSS) at the time of completion.

The Contractor shall inspect the Airport facilities, as provided in **Exhibit B - Reference Documents**, to ensure that there is adequate utility infrastructure and space for the proposed equipment and systems. If additional utilities are required, the Contractor must provide an itemized listing of the required utilities to be included with the proposal along with a fixed price quote for the installation. For the following scoped systems, the Contractor shall clearly identify where a core offering is being proposed and where a subcontractor will be used to prove a system or a service.

The Contractor shall submit a detailed disposal, installation, transition, and implementation plan ("Plan") for the disposal of the existing CUPPS and CUSS systems, installation of the new CUPPS and CUSS system, and transition from the existing systems in two (2) phases to the new CUPPS and CUSS systems while maintaining daily Airport and airline operations. All installations done pursuant to this Contract shall be routine and usual work that is incidental to the replacement of the CUPPS/CUSS equipment.

A. The Plan shall include:

1. List of all CUPPS and CUSS equipment by Terminal building (A, B, C) to be disposed of and to be installed.

2. The network (and server, if required) infrastructure design, including a network diagram.
3. Detailed phasing and timing of installation, transition, and implementation of the new CUPPS and CUSS equipment, hardware, peripherals, associated mounts, associated trays, and software, while accounting for the need to keep the Airport and airlines in operation, for training required, and for transition period(s) between the old and new systems.
4. Training schedule for Airport and airline staff.
5. Current Terminal Buildings
 - a. Terminal A - 18601 Airport Way, Santa Ana, CA 92707
 - b. Terminal B - 18601 Airport Way, Santa Ana, CA 92702
 - c. Terminal C - 18601 Airport Way, Santa Ana, CA 92702

3. COMMON USE PASSENGER PROCESSING SYSTEM (CUPPS)

The existing Common Use Passenger Processing (CUPPS) System, including all hardware, peripherals, displays, mounts, trays, scanners, printers, and software was provided by SITA (formerly Ultra/Materna) in 2011. This existing CUPPS system has been discontinued and is no longer being supported. The County requires a new (cloud based preferred) CUPPS and a new CUSS system that can utilize the existing infrastructure and millwork. The Contractor shall dispose of the existing components, equipment, displays, kiosks, mounts, trays, and software, and install all necessary components including but not limited to equipment, peripherals, displays, workstations, scanners, printers, mounts, trays, displays, kiosks, and software that will enable multiple airlines, ground handlers, or others to share physical check-in or gate podium positions, whether simultaneously, to operate in the facility using their host software and a common set of compatible hardware, without the need for any software or equipment configurations or modifications by any specific airline. The Contractor shall submit a detailed disposal, installation transition and implementation plan (“Plan”) for the disposal of the existing CUPPS and CUSS systems, installation of the new CUPPS and CUSS system, and transition from the existing systems in two (2) phased to the new CUPPS and CUSS systems while maintaining daily Airport and airline operations. The installations of the new CUPPS and CUSS systems shall be routine and usual work that is incidental to the replacement of the CUPPS/CUSS equipment.

The CUPPS compliant platform for Departure Control System (DCS) Applications will support each airline who will be operating on the CUPPS at the Airport at the time of implementation. The CUPPS host interface solution will support existing airlines' connectivity requirements.

The existing CUPPS platform consists of the following:

- A. One hundred twelve (114) ticket lobby check-in counter workstation positions which include computers, displays, printers, 2D handheld boarding pass readers, other peripherals, keyboard and mouse trays, display mounts, and universal power supplies.
- B. Ninety-two (92) gate counter workstation positions which include but are not limited to computers, displays, RFID capable bag tag printers, boarding pass printers, fixed boarding gate readers (BGRs), 2D handheld boarding pass readers, magnetic stripe readers (MSRs), optical character reader (OCRs), keyboards, mice, keyboard and mouse trays, display mounts, a common use digital copier and printer (DCP), and universal power supplies.
- C. Six (6) skycap check-in positions per terminal (18 in total) which include computers, displays, RFID capable bag tag printers, boarding pass printers, magnetic stripe readers (MSRs), optical

character reader (OCRs), 2D handheld boarding pass readers, keyboards, mice, other peripherals, keyboard and mouse trays, display mounts, and universal power supplies.

- D. Four (4) Customs and Border Protection (CBP) international Arrivals Recheck workstations, which include computers, displays, RFID capable bag tag printers, boarding pass printers, magnetic stripe readers (MSRs), optical character reader (OCRs), 2D handheld boarding pass readers, other peripherals, keyboard and mouse trays, display mounts, and universal power supplies.
- E. Eight (8) baggage makeup area CUPPS workstations (2 in Terminal A, 2 in Terminal B, and 4 in Terminal C).
- F. Four (4) Common Use Training & Testing Lab CUPPS workstations, which include components from ticketing, gate counter, and skycap workstations.

4. COMMON USE SELF-SERVICE (CUSS) SOLUTION

Dispose of all existing Common Use Self-Service (CUSS) kiosks that were provided by SITA with a new CUSS solution that will enable passengers to check-in to any airline at any kiosk simultaneously or consecutively without the need for any software or equipment configurations or modifications by any specific airline. Reuse existing power, data, and anchoring bolts if possible.

The existing CUSS platform consists of the following:

- A. One hundred sixteen (116) Check-in Lobby Kiosks
- B. Two (2) Common Use Testing and Lab Kiosk

5. CONTENT MANAGEMENT SYSTEM (CMS)/DIGITAL DISPLAYS

John Wayne Airport (JWA) does not currently have a full feature CMS (Content Management System) and is currently using feeds from the Flight Information Display System (FIDS) and CUPPS platforms to provide digital signage information. The Contractor shall replace this system and implement a new feature rich, flexible, and supportable CMS system to meet airline, airport and passenger needs for displaying visual information into the foreseeable future for the JWA campus, including but not limited to gate information, flight information, baggage information, airline proprietary information including lists such as priority passenger call-up, boarding announcements, or upgrade list information, and code-compliant visual paging system information including emergency broadcast and evacuation messaging, airline standard messages, fully custom messages, passenger messaging/paging call information, and pre-recorded messaging by JWA. The visual paging component must integrate with an existing IED audio paging system and must scroll thru relevant text in synchronization with audio being played over the paging system speakers.

The new CMS shall integrate into and support the County's overall common use environment and approach. The CMS shall give the Airport control over content across all connected devices. Additionally, the Proposed solution should include both a proposed full replacement of all existing displays and an option for reuse of the existing displays. The Airport reserves the right to choose one of these two options. The CMS system shall also be utilized to distribute code-compliant Visual Paging messaging, Department of Homeland Security (DHS)/ Transportation and Safety Agency (TSA) and County proprietary messaging throughout the Airport.

The current information displays and visual paging displays consist of the following:

- Thirty-seven (37) Samsung PM49H 49" visual paging displays (one (1) at each gate 2-21 (total 20), one (1) at each commuter gates 1ABC and 22ABC (total 2), three (3) in the Customs and Border Protection (CBP) Federal Inspection Station (FIS) facility and recheck, one (1) at each checkpoint

Terminal A/B/C (total 3), one (1) at each baggage claim Terminal A/B/C and Terminal C internationals arrivals area (total 4), one (1) in the rotated square between Terminals A and B on Departures deck landside, one (1) at each check-in lobby in Terminals A, B and C (total 3)).

- Eighty-eight (88) Flight Information Displays (FIDS) and multi-use Flight Information Displays (MuFIDS) throughout all Terminals A, B, C and CBP FIS, 50"-57" at the large MuFIDS/directory displays at the ends of each Security Checkpoint in Terminals A, B, C) in size, primarily comprised of Samsung or NEC models.
- Six (6) Multi-Use Flight Information Displays, 60" in size, at sterile ends of each Terminal security checkpoint at the top of each terminal directory board.
- Forty-eight (48) Gate Information Display System (GIDS) displays, 50" in size, primarily comprised of Samsung or NEC models.
- Forty-five (45) of Baggage Information Display System (BIDS) displays, 50" in size, primarily comprised of Samsung or NEC models
 - Sixteen (16) Bag Outbound Makeup BIDS displays across Terminals A, B, C baggage makeup areas, 50" in size, primarily comprised of Samsung or NEC models.
 - Nine (9) Bag Inbound Belt displays across Terminals A, B, and C baggage makeup areas, 50" in size, primarily comprised of Samsung or NEC models.
 - Twenty (20) 24" Carousel Number BIDS displays (one (1) on each gate pylon for Gates 2-21).
- One hundred sixty-two (162) Check-in Backwall displays, 40" in size, primarily comprised of Samsung or NEC models.
- One hundred fourteen (114) Check-in/Ticket Lobby Overhead displays, 40" in size, primarily comprised of Samsung or NEC models.

In addition, JWA has thirty-six (36) Visual Paging displays throughout the JWA campus, driven by the IED/Atlas Public Address System.

The scope of the solution to be provided and configured includes:

- A. Content Management System (CMS)
- B. Content Development for the existing displays
- C. Content Development for future displays
- D. Integration with Resource Management System (RMS)
- E. Integration of a data feed for flight information
- F. Integration with existing IED Atlas Public Address System for Visual Paging
- G. Integration with Baggage Handling System

All replacement digital displays shall meet these minimum requirements:

- A. Displays shall be commercial-grade, 24/7 rated for consistency LED -backlit LCDs with sustained brightness of >700 nits (FIDS, backwalls) and >500 nits (BIDS), anti-glare coatings, >178° viewing, and VESA mounts. Exterior mounted displays shall be commercial grade, 24/7 rated for consistency, LED-backlit LCDs with sustained brightness of >3500 nits in full size, 200 nits under

a roof/canopy, and auto-dimming to 300 nits at night. Exterior displays must also have anti-reflective glass and must be capable of operating under direct sunlight with appropriate visibility.

- B. Units shall provide HDMI 2.0 and DisplayPort inputs, LAN with 802.1X, RS-232C, OPS/SDM slot, input failover, and remove device management via secure HTTP API. If new display units require DDCs to drive content to the displays, Direct Digital Controls (DDCs) shall be power-over-ethernet (PoE) capable.
- C. Color presets shall include D65/Rec.709 with brightness uniformity <+15%.
- D. Devices shall support pixel-shift and panel care to mitigate image retention.
- E. Display backlight life shall be >70,000 hours to L50 measured at the specified calibrated brightness (>600 nits).
- F. Mean Time between failures (electronics) >60,000 hours.
- G. Contractor shall provide brightness maintenance curves vs. ambient temperature.
- H. Power shall be 100-240 V AC with IED C13 and documented typical power at 500 nits.
- I. Compliance: UL/ETL, FCC Class A, RoHS; NDAA/TAA where required.
- J. VESA mount compatible.
- K. Warranty: Minimum three (3) year advanced exchange or on-site.
- L. Existing FIDs, BIDs, and GIDs displays 32"-46" shall be replaced with 50" displays where possible. Existing displays larger than 50" shall be replaced with 60" displays where possible. Display sizes smaller or larger than aforementioned sizes should generally conform to the closest aforementioned sizes where possible to keep the equipment diversity to a minimum. Contractor shall propose alternative sizes if the conditions do not accommodate aforementioned sizes. All displays shall have minimum bezels and shall be installed in close proximity to provide a near-seamless and consistent visual appearance. Manufacturer will guarantee availability of this model for a minimum of three (3) years for any replacements or new additions.
- M. Displays shall reuse existing mounts, where possible. If mounts replacements are required, the Contractor shall immediately notify the County Project Manager of any required changes to the building structure needed to support new mounts before such work is commenced.

6. RESOURCE MANAGEMENT SYSTEM (RMS)

JWA currently operates a SITA Resource Management System (RMS) as part of their existing CUPPS platform. A replacement platform shall be provided, either by the primary Contractor or by a subcontractor. The system shall provide a rules-based solution which allows for granular Airport management of gate assignments.

7. EXISTING CABLING AND ELECTRICAL INFRASTRUCTURE

JWA requires that a survey of existing cabling and electrical infrastructure shall be conducted after award to determine if changes are needed to support the desired functionalities and implementation of the new systems, specifically with the cabling and electrical needs. This survey walk may need to include tracing and testing of existing lines. Any changes to existing infrastructure shall be proposed before the implementation process.

8. OPTIONAL SCOPE - LOCAL DEPARTURE CONTROL SYSTEM (LDCS)

JWA currently does not operate a Local Departure Control System (LDCS). The Airport is requiring a proposal to include details and cost on an LDCS as an optional scope item.

9. SUPPORT SERVICES

The Contractor shall provide Support Services for all installed hardware, peripherals, and software for three (3) years with an option to renew for two (2) years. See Maintenance and Support Requirements under Section 23.

10. PROPOSED SYSTEM - GENERAL REQUIREMENTS

The following requirements apply to all proposed systems:

- A. The successful Contractor will provide a hosted solution. Regardless of the architecture and physical location, the Contractor is required to operate, manage and maintain the entire system.
- B. Contractor shall furnish, all design, development, hardware, firmware, software, licenses, integration, implementation, labor, material, equipment and other associated components to complete all systems implementation.
- C. Both Ticket-Counter and Self-Service Kiosks shall be capable of accepting mag strip, encrypted, and proximity, payments. All accessories associated with payment types shall be included as part of the unit.
- D. Contractor shall propose a complete turn-key system, including all hardware, software, printers and other peripherals. The network will be provided by County as described in this RFP.
- E. Installed equipment shall not be set to operate at over 70% capacity for durations exceeding fifteen (15) minutes.
- F. Contractor shall provide a detailed network diagram of the systems, detailing all connections, interchange points with airlines, and integrations with other systems. The diagram shall also include what ISP configurations and IP address assignments are necessary for the deployment of all systems. Network design and IP address assignments must be coordinated with JWA and adhere to County standards.
- G. Contractor shall provide redundant connections to the systems. The Contractor shall explain any concerns with providing this redundancy.
- H. Contractor shall provide a dedicated environment exclusively for JWA. The Contractor must ensure and demonstrate that JWA's data is fully segregated and not comingled with the data of any other customers.
- I. The Contractor shall describe how their system handles airline mobile processing systems (such as airline agent use of tablets, phones, handheld devices).
- J. Contractor shall provide JWA with three environments: Production, Testing, and Training.
- K. The Proposed systems shall be designed with the redundancy and resiliency required for maximum uptime (100%) with same or better airline response times.
- L. The Contractor shall model all assets impacted by the solution implementation to define level of development (LOD 400) while meeting JWA BIM Standards.
- M. The Contractor shall provide solutions utilizing current operating systems that comply with International Air Transport Association (IATA) and Payment Card Industry Security Standard (PCI

DSS) standards. The Contractor shall detail the measures and processes that will be implemented to ensure ongoing compliance.

- N. The Contractor shall provide detailed information on alternative payment methods currently deployed at other airports that do not utilize the airport's network to transmit sensitive payment information.
- O. Where any requirement conflicts with other requirements, the more stringent will apply.

11. CUPPS GENERAL REQUIREMENTS

The County prefers a cloud-hosted system to meet the needs, as outlined in this RFP. Assuming all requirements are met equally, the ability to provide a cloud system will be preferred.

- A. Contractor shall provide a system that meets the current IATA CUPPS standard at time of proposal.
- B. Contractor shall describe the high-level features and functionality of the system.
- C. Contractor shall describe how the system servers can be hosted in the Cloud.
- D. If the Contractor cannot provide system servers that can be hosted in the Cloud, describe how the system servers can be managed On-Premises.
- E. Contractor shall provide a description and diagram of proposed airline connections. This should include any backup connections that will be provided.
- F. If Contractor cannot provide airline connections hosted in the Cloud, describe how the airline connections can be configured and managed On-Premise.
- G. Contractor shall clearly define which operations/servers/etc. are done on site versus in the cloud hosted environment.
- H. Contractor shall provide a system architecture in Visio and PDF formats. **(Provide as Appendix A– CUPPS Architecture Diagram)**
- I. Contractor shall provide pricing for the system in at least one of the following deployment options:
 - 1. Full Cloud/Hosted Solution - Represents the CUPPS Platform being installed in the Cloud and the airline connections hosted and managed in the Cloud. (Pricing for a Full Cloud/Hosted Solution shall be provided in the Pricing Proposal).
 - 2. Cloud CUPPS with On-Premise airline connections - Represents the CUPPS platform being installed in the Cloud and the airline connections managed On-Premise. (Pricing for Cloud CUPPS with On-Premise Airline Connections shall be provided in the Pricing Proposal)
 - 3. On-Premise CUPPS with hosted airline connections - Represents the CUPPS Platform being installed On-Premise and the Airline Connections hosted and managed in the Cloud. (Pricing for On-Premise CUPPS with hosted airline connections shall be provided in the Pricing Proposal)
 - 4. Full On-Premise Solution - Represents the CUPPS Platform being installed On-Premise and the airline connections managed On-Premise. (Pricing for a Full On-Premise Solution shall be provided in the Pricing Proposal)
- J. Contractor shall describe the necessary network configuration, including equipment, to be deployed onsite at JWA, to enable communications to the system servers and airline hosts.

- K. Contractor shall state the minimum hardware configuration for any other equipment required onsite at JWA for the system, including all the applicable cabling connections.
- L. Contractor shall provide redundant connections to the system. The Contractor should describe how the system can track the history of availability.
- M. The Contractor shall explain how they will support a certified Departure Control System (DCS) Application for each airline who will be operating on the CUPPS at the Airport at the time of implementation. Any airline who currently has a CUPPS certified application shall incur no additional charges for certification or deployment.
- N. Contractor shall provide a CUPPS Platform that provides backward compatibility to legacy airline common use applications.
- O. Contractor shall explain how they will accommodate new airlines onto the CUPPS platform. Any costs associated with new airline accommodations shall be included in the Pricing Proposal.
- P. Contractor shall explain how the system can accommodate growth (e.g., expanding to other gates/locations) and changes to the business model without negative impact to performance.
- Q. Contractor shall describe how they meet the following requirements:
 - 1. Devices within a CUPPS Platform shall only be used by applications initiated and operated with the platform or diagnostic software.
 - 2. Contractor shall be responsible for the delivery of platform functionality required to support the business applications and processes of its users.
- R. The Contractor shall provide a CUPPS host interface solution to support existing airlines' requirements for connectivity to their DCS, as well as accommodate new entrant airlines in the Airport quickly. All coordination of activities and agreements for use shall be the responsibility of the Contractor in coordination with JWA.
 - 1. The Contractor shall provide an annual licensing agreement for the CUPPS application that is consistent with the initial capacity and expansion capability requirements.

12. COMMON USE SELF SERVICE (CUSS) REQUIREMENTS

The County prefers a cloud-hosted system capable of meeting, at a minimum, the following requirements as outlined below:

- A. Contract shall provide a system that meets the most current IATA CUSS 2.0.x or newer standard at the time of proposal.
- B. Contractor shall describe the high-level features and functionality of the system.
- C. Contractor shall describe how the system servers can be hosted in the Cloud.
- D. If the Contractor cannot provide system servers that can be hosted in the Cloud, describe how the system servers can be managed On-Premises.
- E. Contractor shall describe how the airline connections can be hosted in the Cloud.
- F. If the Contractor cannot provide airline connections hosted in the Cloud, describe how the airline connections can be configured and managed On-Premises.
- G. Contractor shall provide a system architecture diagram in Visio and PDF formats. **(Provide as Appendix B - CUSS Architecture Diagram).**

- H. Contractor shall provide a certified CUSS Application for each airline who chooses to utilize CUSS at the Airport at the time of implementation.
- I. Contractor shall be responsible for implementing airline CUSS applications up to and until final systems acceptance for all the CUSS participating airlines currently operating out of JWA.
- J. The implementation shall include up to one hundred sixteen (116) check-in lobby kiosks and one (1) common use testing and training lab kiosk and the full number of current participating airlines operating out of JWA. The installed system shall be capable of adding additional kiosks, as the need arises, without negative impact to performance.
- K. The Airport reserves the right to purchase less than one hundred sixteen (116) CUSS kiosk units. The Contractor shall provide unit costs for the kiosks. (Pricing Proposal)
- L. Contractor shall provide an annual licensing agreement for the CUSS that is consistent with the initial capacity and expansion capability requirements.

13. CONTENT MANAGEMENT SYSTEM (CMS) REQUIREMENTS

- A. The Contractor shall provide a CMS to enable content on the JWA information display screens (xIDS):
 - 1. Flight information (FIDS/MUFIDS) shall provide a display of upcoming flights with their associated gates, schedules, and present status.
 - 2. Gate information (GIDS) shall provide gate-specific flight information, urgent alerts, and other information as required by County or airline staff (e.g. flight boarding information, upgrade lists, standby lists, fully custom messages, emergency and evacuation messaging, and other airline and airport industry standard messaging).
 - 3. Baggage information (BIDS) shall provide baggage carousel assignment per flight and other pertinent information.
 - 4. Baggage Carousel Display shall provide baggage carousel information to passengers deplaning aircraft at the gate on the jet bridge-facing side of the gate pylon.
- B. The system shall enable flight information for airlines at JWA to be populated and updated automatically via JWA's flight view data source.
- C. The system shall enable flight information to be displayed on monitors to be located throughout the Airport for a total of three hundred fifty (350) displays.
- D. The Display System shall allow basic configuration through a current and supported web browser.
- E. System shall have access control with adjustable permissions and logging.
- F. System shall be able to export live data to be displayed on the Airport's display system.
- G. System shall have display interfaces that are remotely configurable and only require power and network connectivity to function. Power over Ethernet (PoE) is preferred.
- H. System shall be simple and intuitive so that the appropriate airline employees can view or modify information with little training.
- I. System shall have the ability to display data in multiple languages.

- J. The Contractor shall describe the process for creation of content, both and initial set and future sets of needed content. This should include any needed meetings between Contractor and Airport, samples needed from Airport, and any other needed items.
- K. The Contractor shall describe how the CMS solution enables text, graphical, and video-based messaging to be dynamically assigned to designated video monitors throughout the Airport campus.
- L. The system shall enable content display and creation that meets current ADA requirements. The Contractor shall describe how the CMS will meet these requirements, such as text size, color, height, etc. and explain if there is a feature that will warn a user if they attempt to enter non-ADA compliant custom content.
- M. Contractor shall describe how the CMS will provide content type prioritization to enable takeover for specific terminal information, weather alerts, or safety and security instructions. Emergency messaging must be able to be activated by all JWA user accounts and be able to be displayed over all other content, until deactivated by the JWA user.
- N. Contractor shall provide a CMS that will support enhanced capabilities, such as:
 - 1. Full HD Video
 - 2. Website Feeds
 - 3. Interactive Wayfinding and Navigation
 - 4. Visual Paging
 - 5. Display of GIDS through a URL (use by airlines)
 - 6. Time-sensitive messages and emergency messaging
- O. Contractor shall explain how the CMS can provide templates for displaying content consistently throughout the Airport, with Airport specific branding.
- P. Contractor shall explain how the CMS can provide for the grouping of devices/displays by zone, purpose, type; to enable specific content to be pushed to displays in those categories.
- Q. Contractor shall explain how the CMS can provide for the scheduling of content to be displayed in sequence, at specific times/locations.
- R. Contractor shall explain how the CMS can prioritize role-based access control to restrict editing capabilities to specific zones or displays based on operational needs.
- S. Contractor shall explain how the CMS can be utilized to display sensitive, time-based, content across multiple displays or zones in an emergency situation.
- T. Contractor shall explain how the CMS, as installed, will be capable of expanding to other JWA controlled displays throughout the airport campus by adding resources as required, without negative impact to performance.
- U. Contractor shall describe the licensing agreement for the CMS application that is consistent with the initial capacity and expansion capability requirements.
- V. Contractor shall provide a system architecture in Visio and PDF formats. **(Provide as Appendix C - CMS Architecture Diagram)**

14. **ARLINE APPLICATION CERTIFICATION**

- A. The Contractor shall certify that they currently support the following airlines operating at JWA.

*County of Orange
John Wayne Airport*

*Common Use Passenger Processing (CUPPS) and
Common Use Self Service (CUSS) Systems Replacement
& Support Services*

*Page 72 of 106
2928904*

1. Arline Air Canada (AC)
2. Alaska Airlines (AS)
3. Allegiant Air (G7)
4. American Airlines (AA)
5. Breeze Airways (MX)
6. Delta Airlines (DL)
7. Frontier Airlines (F9)
8. Southwest Airlines (WN)
9. Spirit Airlines (NK)
10. United Airlines (UA)
11. WestJet Airlines (WS)

- B. Contractor shall describe any costs to the County or the airline to certify an airline after implementation (Pricing for certification after implementation shall be provided in Pricing Proposal).

15. AIRLINE DEPARTURE CONTROL SYSTEM (DCS) CLOUD CONNECTIVITY

- A. Contractor shall certify that they support DCS for the following airlines.
1. Airline Air Canada (AC), Alaska Airlines (AS), Allegiant Air (G7), American Airlines (AA), Breeze Airways (MX), Delta Airlines (DL), Frontier Airlines (F9), Southwest Airlines (WN), Spirit Airlines (NK), Skywest Airlines (OO), United Airlines (UA), and WestJet Airlines (WS).
- B. Contractor shall describe any costs to the County or the airline during implementation to establish a new connection in the Cloud after implementation. (Pricing for DCS connectivity shall be provided in Pricing Proposal).

16. RESOURCE MANAGEMENT SYSTEM (RMS) REQUIREMENTS

- A. The Contractor shall provide RMS solution that provides the following features:
1. RMS includes Real Time Data into the system to produce a gate plan (Gantt chart) based on airport-specific rules.
 2. Contractor shall offer the creation of a centralized data base with flight schedules.
 3. Ability for the system to alert when a gate conflict is created and capable of reallocating gate assignments from one gate to another via a drag/drop method.
 4. Query tool for historical flight data/gate utilization information.
 5. Ability to manually input ad-hoc charter flight information for display on gate Gantt chart.
 6. Ability to manually upload a flight schedule.
 7. Ability to simulate gate assignment scenarios for future planning (preferably ninety (90) days out)
 8. Ability to change the rules per gate within the system.

9. Automatic warning when rules are broken.
 10. Ability to add or remove gates and add remote hardstand areas to show in the system's Gantt chart.
 11. Unlimited user log in. Secure and tiered security access allowing JWA and airline access if required. Gate Request function allows all users in the Gate Management process to collaborate seamlessly in using shared resource. It enables an operator to "request" the usage of Gate from its owner and for the Owner to either accept or reject that request with a reason.
 12. Map based view showing gate assignments in real time over a 24-hour period.
 13. Forecast tool and future stand planning. Preferably ninety (90) days out.
 14. Stand outage management and planning of outages shown within the system for scheduled closures or temporary maintenance.
 15. Tow Management allows airport to define and readily set up tows against specific flights and allocations using simple point and click on the Gantt chart.
 16. Ability to run the gate utilization report.
 17. Ability to show canceled and diverted flights in Gantt chart.
- B. The Contractor shall provide a system architecture diagram in Visio and PDF formats. **(Provide as Appendix D- RMS Architecture Diagram).**

17. VISUAL PAGING REQUIREMENTS

Visual paging messaging shall be compliant with all applicable codes and regulations (e.g. Americans with Disabilities Act, California Building Code, etc.) and must be inspected and approved by a California Certified Accessibility Specialist (Caspi) for compliance with all applicable codes, regulations, and ordinance for properties including but not limited to screen placement (including distance from next visual paging display and mounted height/distance from finished floor), character height above finished floor, character size for appropriate visibility from distance, and synchronized audio and text output between the audio paging and visual paging systems. Control/input interface shall be from every CUPPS workstation (including ticket lobbies, gates, and skycap) in Terminals A, B, and C, Orange County Sheriff Dispatch, Airport Maintenance Service Desk, and all information booths (one in each Terminal A, B, and C baggage claims).

18. HARDWARE AND SOFTWARE REQUIREMENTS

A. STANDARD REQUIREMENTS

1. Various publications form a part of this specification. Reference most recent version of the below publications for Project adherence includes those listed below and those listed in other parts of the RFP's supporting sections. Contractor shall certify their compliance with the latest versions of the below publications.
 - ISO 9001, 9002, 9003, 9004; Quality Assurance
 - National Electrical Manufacturers Association (NEMA)
 - NFPA 70 National Electrical Code (NEC)
 - IATA Resolution 740; Form of Interline Baggage Tag
 - IATA Resolution 792; Bar Coded Boarding Pass

- IATA RP 1740a; Form of Interline Baggage Tag
 - IATA RP 1796; Baggage System Interface
 - IATA RP 1797; Common Use Passenger Processing System (CUPPS)
 - IATA RP 1706c; Common Use Self-Service (CUSS)
 - IATA RP 1706e; Paper specifications for documents to be printed by a general-purpose printer in a CUSS kiosk
 - A4A RP 30.201
 - ACI RP 500 A07
 - PCI Data Security Standard (PCI DSS)
2. Proposed platform shall include costs and requirements necessary to maintain compliance and certifications with current industry standards, at the time of proposal.
 3. All documentation prepared by the Contractor shall be reviewed by JWA or JWA representative and shall be retained by JWA upon approval.
 4. Software used for this project shall have been developed using revision numbering and tracking procedures. The Contractor shall provide the version numbers for all software being deployed.
 5. Software development shall be completed and documented by developers using internationally recognized computer languages and techniques, and Secure Software Development Lifecycle (SDLC) methods to meet PCI DSS requirements.
 6. Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all County of Orange Information Technology Security Standards ("Security Standards"), as existing or modified, that pertain to Contractor in connection with the Services performed by Contractor as set forth in the scope of work of this Contract. Any violations of such Security Standards shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Standards include, but are not limited to **Exhibit A - JWA Standards Package**.
 7. Adhere to JWA standards. (**See Exhibit A - JWA Standards Package**)
 8. Contractor shall adhere to all applicable laws. The latest version of all documents shall be utilized.
 9. Contractor shall comply with all applicable Federal, State, and local codes and regulations.

B. GENERAL HARDWARE AND SOFTWARE REQUIREMENTS

1. All equipment shall be new and unused and of the Manufacturers Current Model Year and shall include all standard equipment as advertised by the Manufacturer. All equipment listed herein shall comply with Federal, State, and local regulations at the time of delivery.
2. All hardware and software shall be acquired from Contractor authorized resellers or original equipment manufacturers (no grayware).
3. Contractor shall provide a comprehensive list of software licensing agreements required to implement the system based on the requirements, number of servers, number of users, number of workstations, and number of devices to be implemented. Continuous software maintenance on server and endpoints to include all application and security updates.

4. The quantities of licenses must support all the production, testing and training environments. The product name and version shall be clearly defined. The license(s) should be a perpetual enterprise wide license and not be restricted by number of users, devices, servers, etc. All license restrictions must be defined. The list must include both the Contractors' product application licenses and Commercial off the Shelf (COTS) licenses required to implement the system.
5. Equipment shall be rated for continuous use 24 hours a day, 7 days a week.
6. The proposed system shall be scalable to onboard additional applications and modules as the needs of the County or airlines evolve.
7. All CUPPS, CUSS, CMS and RMS equipment will be configured to auto power on after restoration of power. UPS shall be able to power system for up to thirty (30) minutes of runtime after power loss and automatic shutdown at fifteen (15) minutes post loss.
8. The Contractor shall provide 10% spares of all equipment.
9. Contractor shall maintain a current and accurate inventory of all hardware, software, and configuration items in accordance with Information Technology Information Library (ITIL) best practices.

C. CUPPS HARDWARE REQUIREMENTS

1. The Contractor shall provide the following hardware, as required to support the overall CUPPS implementation:
 - a. Servers consistent with the CUPPS technical specification (CUPPS TS), as required by the proposed solution.
 - b. Workstations (computer and monitor) consistent with the CUPPS TS, as required by the proposed solution.
 - c. Network appliances consistent with the CUPPS TS, as required by the proposed solution.
 - d. Hardware that supports the use of Radio Frequency Identification (RFID) bag tags.
 - e. Peripheral devices consistent with IATA Technical Peripheral Specifications (ITPS) formerly the AEA Technical Specifications.
 - i. Standard keyboards and pointing devices for all workstations
 - ii. Boarding pass printers for all workstations
 - iii. Bag tag printers for all workstations, including RFID capability
 - iv. Document printers for all workstations, including RFID capability
 - v. Magnetic stripe reader/optical character recognition (MSR/OCR) scanners for all workstations
 - vi. Chip/PIN readers (optional)
 - vii. 2D barcode scanners for all workstations
 - viii. APC or Vertiv brand (JWA Preference) UPS for all workstations, capable of keeping workstation and connected peripherals up for a minimum of thirty (30) minutes
 - ix. Height/Tilt adjustable monitor/keyboard trays

- x. Boarding Gate Readers (BGR)
- 2. The Contractor shall describe and provide the proposed configuration of devices and peripherals of the CUPPS. **(Provide as Appendix E – CUPPS Configuration Diagram)**
- 3. The Contractor shall ensure equipment dimensions fit within the existing millwork. **(Provide as Appendix F – CUPPS Millwork Diagram)**

D. CUSS HARDWARE REQUIREMENTS

- 1. The Contractor shall provide the following hardware, as required to support the CUSS:
 - a. Peripheral devices consistent with IATA Technical Peripheral Specifications (ITPS) formerly the AEA Technical Specifications.
 - b. All required components, such as workstations, monitors, MSR/OCR scanners, credit card reader, boarding pass printers, and bag-tag printers, and a UPS.
 - c. Servers as required to support the proposed system.
 - d. Hardware that supports the use of RFID bag tags.
 - e. Network appliances as required to support the proposed system.
 - f. Ancillary appurtenances required to support the proposed system.
 - g. Millwork finishes and/or kiosk wrap changes, as coordinated with JWA.
- 2. The Contractor shall reuse existing kiosk anchor bolts and poke-thrus for anchorage and power/data provision, where possible. The Contractor shall notify the County in writing of any inability to reuse existing anchor bolts, poke-thrus, and associated power/data.
- 3. The Contractor shall describe and provide the proposed configuration of devices and peripherals of the CUSS kiosk. **(Provide as Appendix G – CUSS Kiosk Diagram)**
- 4. Automated kiosks shall meet requirements of FAA AC 150/5360-14A, with 100% of the kiosks meeting the CBC accessibility standards.

E. CMS HARDWARE REQUIREMENTS

- 1. The Contractor shall provide full replacement of all existing digital displays and an option for reusing existing displays. Costing for both shall be provided within the Pricing Proposal.
- 2. For new displays, the Contractor shall provide costing using the following requirements:
 - a. Designed to be as close to one-to-one match to existing displays as possible (size and quality), while meeting the requirements detailed in section 3.5 Content Management System (CMS) /Digital Displays.
- 3. The Contractor shall additionally provide the following hardware, as required to support the CMS:
 - a. Servers as required to support the proposed system.
 - b. Direct Digital Control (DDC), PC, or Video Players as required to support the proposed system.
 - c. Network appliances as required to support the proposed system.
 - d. Ancillary appurtenances required to support the proposed system.

4. The Contractor shall describe and provide the proposed configuration of devices for the CMS. **(Provide as Appendix H – CMS Displays Diagram)**
5. DDCs that support power over Ethernet (POE) are required.

F. CYBERSECURITY REQUIREMENTS

1. County of Orange Information Technology Security Standards: County of Orange security standards follow the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.
2. The Contractor shall provide technology solutions that support the Airport's cybersecurity policies, procedures, plans, and guidelines for protocols, configurations, software development, governance, risk identification, recovery methods, incident response, and protection of Airport assets. Contractor shall provide all support required to fulfill the Airport's commitment to cybersecurity rules, regulations, mandates, and industry best practices, including local, state, and federal.
3. For systems that process credit cards, the Airport requires strict compliance with all elements of cybersecurity, including, but not limited to, Payment Card Industry Data Security Standard (PCI DSS). Contractor shall support all audits as necessary and provide all required remediation or other approved risk mitigation measures to satisfy audit findings. The Airport and the Contractor will develop a mutually acceptable approach for remediation and risk mitigation prior to commencement. Failure to achieve or maintain compliance will result in actions governed by terms of the contract.
 - The system must be certified to the most current version of PCI DSS available by final acceptance of the system, by either the vendor's independent and mutually agreed upon (with County) Qualified Security Analyst (QSA) or by Airport provided Qualified Security Analyst (QSA). Costs for both options shall be provided. The certification must be site-specific to the system installation at the Airport. All systems/devices that scan/transmit credit data, such as Pin Transaction Security, Point of Interaction, and Point of Sale devices, must be PCI DSS certified. All service providers must provide any and all required assistance during the County's PCI DSS audit to obtain an Attestation of Compliance by the Airport. Alternatively, service providers shall include within the proposal costs to independently obtain and provide the PCI DSS audit and Attestation of Compliance for the Airport on an annual basis.
 - The system, its components, and any other systems that process credit card data and integrate with the system must comply with the most current version of the PCI DSS standards by final system acceptance.
 - Vendor's system must be certified by an independent QSA, provided by the vendor. Vendor will perform quarterly audits as required by the PCI DSS standards to remain compliant.
 - Following the implementation of new releases that affect PCI DSS of the CUPPS and CUSS solutions during the term of the contract, the Vendor must recertify the system on-site to be PCI DSS certified, with proof of an Attestation of Compliance. Vendor will recertify PCI DSS for CUPPS and CUSS solution when new PCI DSS versions are released by the time of final acceptance.
4. The Contractor shall provide appropriate evidence for County to achieve compliance of the Contractor's system with the current Payment Card Industry Data Security Standards ("PCI DSS") as may be amended or replaced from time to time.

5. The Contractor shall thoroughly describe its position with regard to PCI DSS, including Chip and PIN. The Contractor shall also describe its approach to ensuring that JWA will not be held liable for violations of the PCI DSS relative to the CUSS Kiosks and the CUPPS platform.
6. Contractor shall satisfy all applicable program or project-related requirements for documentation, submittals, safety, quality, and other related materials in pursuit of successfully meeting all cybersecurity requirements for the proposed system(s).
7. The Contractor shall provide a comprehensive description of its methodology for the proposed systems including, but not limited to, the following elements:
 - a. Risk Categorization by System
 - b. Process Controls for each Risk Categorization
 - c. Specifications and Software Development as required to accomplish Process Controls.
 - d. Airport Network Requirements
 - e. Physical Security and Access Control
 - f. Passwords, Service Accounts and Credential Use Policies
 - g. Antivirus and Related Malware Defenses
 - h. Patch Management of all firmware and software, including head end and edge devices, peripherals, controllers, operating systems, proprietary applications and COTS applications.
 - i. Data Protection
 - j. Payment Card Industry Data Security Standard (PCI DSS) Compliance
 - k. Audit and Monitoring
 - l. Training and Awareness
 - m. Successful Proposer will develop a plan for Cybersecurity and follow the project's submittals' guidelines for approval.
 - n. Software Bill of Materials for Contractor developed/utilized software and drivers.
8. The Contractor shall include all cybersecurity related costs in the Pricing Proposal.
9. The Contractor shall comply with all cybersecurity requirements in the County IT Standards. **(See Exhibit A- JWA Standards package).**

19. SYSTEM INTERFACES/INTEGRATIONS

A. CUPPS INTERFACES

1. The Contractor shall provide integrations between CUPPS and CMS resulting in functionality that:
 - a. Allows users to interact with the CMS, from a CUPPS workstation, to manually trigger signage to reflect operationally related, airline content on appropriate displays that have been linked to the operations occurring at the CUPPS workstations (First Class, Bag drop, Boarding Sequence, etc.).

2. The Contractor shall provide the ability to launch the Airport RMS through a web browser from the CUPPS workstation.
3. The Contractor shall provide the CUPPS interface architecture for all interfaces. (**Provide as Appendix I - CUPPS Interface Diagram**)
4. The Contractor shall provide the ability to add integrations for Airline back office systems or other JWA applications (generally open architecture).

B. CMS INTERFACES

1. The Contractor shall provide integrations between CMS and CUPPS resulting in functionality that allow for:
 - a. Ability to interact with the CMS, from a CUPPS workstation, to manually trigger signage to reflect operationally related, airline content on appropriate displays that have been linked to the operations occurring at the CUPPS workstations (First Class, Bag drop, Boarding Sequence, etc.)
 - b. Add custom text messages to be displayed.
 - c. Ability to display template text messages provided by the County, airlines, and Law Enforcement.
2. The Contractor shall provide integrations between CMS and Baggage Input Console (BIC) resulting in functionality that:
 - a. Carousel assignments as determined by airline personnel interacting with the BIC. The CMS shall be able to receive carousel assignment information from the Baggage Handling System, and in-turn display the appropriate Flight and Baggage information on the assigned bag claim carousel displays and any other Baggage Information Displays (BIDS).
3. The Contractor shall provide integrations between CMS and JWA'S RMS resulting in the following functionality:
 - a. The CMS shall receive flight data and resource assignment information managed in the RMS. Any updates to flight-related information coming from the RMS, shall take priority over the information received through other automations, such as flight feeds, etc.
4. The Contractor shall provide integrations between CMS and IED Atlas Public Address System for Visual Paging resulting in the following functionality:
 - a. The CMS shall be capable of receiving a text string for Visual Paging to accompany an audible message. Once the string is received, it can be displayed on any or all Visual Paging displays.
 - b. Scheduling visual paging to be in sync with audio paging.
5. The Contractor shall describe how the CMS will send/receive information to/from all interfaced systems.
 - a. This shall include all workstations, Airport Police Services, and Airport Maintenance Service Desk.
6. The CMS shall provide an open application programmable interface (API) to add additional content providers as required by JWA.

7. The Contractor shall provide CASp certification of compliance with pertinent Federal, State and local codes and regulations.
8. The Contractor shall provide the CMS interface architecture for all interfaces. **(Provide as Appendix J – CMS Interface Diagram)**

C. RMS INTERFACES

1. The Contractor shall provide the RMS interface architecture for all interfaces. **(Provide as Appendix K – RMS Interface Diagram)**
2. The Contractor shall provide an integration to the CMS. For example, display information at a specific asset should match the assigned user.
3. The Contractor shall provide an integration with the flight information feed.
4. The Contractor shall provide an integration with BHS (dynamic bag claim assignments and content displays in baggage areas).

D. ASSET MANAGEMENT INTERFACES

1. The Contractor shall provide a method of integration with the Airport's asset management solution to automatically import and maintain a current inventory in the latter system (for future integration).
2. The Contractor shall provide to the Airport an asset inventory in compliance with PCI DSS, including make, model, unique identifier (e.g. serial number), location, for inclusion into a future County asset management solution.

20. SYSTEM REQUIREMENTS

- A. LICENSING - The County prefers and annual licensing agreement for the proposed platform that is consistent with the initial capacity and expansion capability requirements.
 1. The Contractor shall provide pricing for licensing in the Pricing Proposal.
 2. The Contractor shall explain the licensing structure for the CUPPS, CUSS and CMS and RMS (e.g., Enterprise/Site/Per User).
 3. The Contractor shall explain how to accommodate any changes to the business model including an increase in gate operations or number of users.
 4. The Contractor shall accommodate at least two major platform updates within the scope of this agreement, at no additional cost, upon notification from the County.
- B. DISASTER RECOVERY - The Contractor shall indicate the capability to recover from natural, human-caused, and electronic disasters (including security compromises) that could interrupt service to JWA and its customers. The Contractor shall describe their system including:
 1. Procedures for off-site storage of information.
 2. Capabilities and availability of alternate processing, communications, and operations facilities.
 3. Plans for maintaining business processes, including communications with JWA, its customers, and suppliers of goods and services.
 4. Estimated time to recover from disaster events, and service level expectations for business continuity following a disaster.

5. Cost to JWA, if any, for disaster recovery services. (Pricing for Disaster Recovery shall be provided in Pricing Proposal)
6. A documented disaster recovery and business continuity plan, including dates of disaster recovery tests and schedule for future tests.

C. SYSTEM MONITORING

1. The Contractor shall describe any monitoring tools to report status, health, or system level performance. Include explanation of any real-time monitoring and alert notifications.
2. The Contractor shall describe the means for monitoring endpoint devices.
3. The Contractor shall describe how the systems can monitor peripherals (e.g., status, out of paper).
4. The Contractor shall describe how the systems log and report system events and faults.

D. CUPPS REPORTING

1. The system shall provide standard reports. The system shall be capable of providing historical reports on all of the real-time monitored components mentioned in System Monitoring Section. The Contractor shall provide a sample of the standard reports.
2. The Contractor shall provide a dashboard/portal to airport IT for viewing status of devices and peripherals. The dashboard/portal shall also have alert capabilities for when devices are low on consumables or need support. Airport IT shall have the ability to see which devices are in need of support.
 - a. The proposed solution shall provide **Summary Activity** data such as:
 - Login
 - Workstation Activity
 - Logout
 - Printing Transaction
 - b. The proposed solution shall provide **Login Activity** data such as:
 - Carrier
 - User/Arline (this may be a generic airline user id)
 - Date and Time
 - Workstation
 - c. The proposed solution shall provide **Workstation Activity** data such as:
 - Applications launched
 - Date and Time Applications were opened
 - Date and Time Applications were closed
 - Workstation Status (online/offline)
 - d. The proposed solution shall provide **Logout Activity** data such as:

- Carrier
 - User/Airline (this may be generic airline user id)
 - Date and Time
 - Workstation
3. The proposed solution shall provide **Printing Transactions Activity** data such as:
 - Carrier
 - User/Airline Account
 - Date and Time
 - Type (boarding pass, bag-tag, etc.)
 - Quantity of each type of print
 - Workstation
 4. The proposed solution shall provide **Data Standards** to be deployed and if/how they meet the following requirements:
 - The database shall be designed in accordance with industry standards for an open database platform
 - The database platform shall be the latest version available at the time of the project award
 - The database shall comply with Open Database Connectivity (ODBC) interface practices
 5. The proposed solution shall provide **Data Sharing** and if/how they meet the following requirements:
 - The database shall be a common relational database, capable for use by the subsystems
 - Any database information shall be available based on and according to specific user authorizations and in accordance with security requirements
 - Data export features for other business unit use and reporting
 6. The proposed solution shall provide **Data Integrity** and if/how they meet the following requirements:
 - The database shall be equipped with real time backup of live data and restoration protocol to assist in disaster recovery
 - The database shall have an approved storage and archival functionality
 - Data Security shall be further defined by the selected Contractor and approved by JWA
 7. Contractor shall describe how the system supports ad-hoc queries.
 8. The Contractor shall describe how the system supports web-publishing using a COTS report engine.

E. CUSS REPORTING

1. The system shall provide standard reports. The Contractor shall provide a sample of the standard reports.

2. The proposed solution shall provide Workstation Activity data such as:
 - Applications Launched
 - Date and Time Applications were opened
 - Date and Time Applications were closed
 - Workstation
3. The proposed solution shall provide Printing Transactions Activity data such as:
 - Carrier
 - User/Arline Account
 - Data and Time
 - Type (boarding pass, bag-tag, etc.)
 - Quantity of each type of print
 - Workstation
4. The Contractor shall describe how the system support ad-hoc queries.
5. The Contractor shall describe how the system supports web-publishing using a COTS report engine.

F. CMS REPORTING

1. The system shall provide standard reports. The Contractor shall provide a sample of the standard reports.
 - Content Displayed
 - Date, Time and Duration of Content on Displays
 - Display ID
2. The proposed solution shall provide **Display or Campaign Activity** data such as:
3. The Contractor shall provide a list of all other data provided in CMS reporting.

G. RMS REPORTING

1. The RMS shall provide the following reporting capabilities:
 - Provide standard reports
 - Provide custom report writing tool
 - Ability to access all rata data for custom reports
 - Provide real-time and on-demand generation of standard and custom reports
 - Ability to export reports/report data
 - Ability to schedule and publish read only standard and custom reports
 - Ability to use an existing standard report as a baseline to build a custom report
 - Ability to report on data from custom fields

- Ability to restrict report access based on role permission
2. The system shall provide interactive dashboard functionality:
 - Provide standard widgets
 - Ability to customize widgets
 - Provide near real-time updates
 - Ability to restrict dashboard access based on role permission
 3. The system shall provide logging and audit trail:
 - Record and archive data in a user searchable format with the ability to generate reports using any parameter recorded
 4. The system shall provide aerial map view with real time updates:
 - Provide ability to "playback" a previous period
 5. The system shall provide resource billable usage functionality:
 - Ability to track and report billable usage
 - Ability to report billable usage in detail and in summary
 - Ability to report billable usage by airline or resource
 - Ability to export billable usage
 - Ability to track cap fee usage
 6. The system shall provide resource and duration reports for:
 - Counters
 - Baggage Claims
 - Baggage Makeup
 - Tows
 - Remote Parking/RONs
 - Gate/Stand Parking
 7. The system shall provide ability to compare actual usage vs scheduled usage.

21. PROJECT EXECUTION AND IMPLEMENTATION REQUIREMENTS

A. SYSTEM DESIGN

1. The Contractor shall supply all system design activities and shall work with the County Project Manager and airlines to complete the final design as specified in this RFP.
2. Prior to the execution of any installation tasks, the Contractor shall submit its final design to JWA for approval.
3. Upon review of the final design by JWA, the Contractor shall be solely responsible for successfully implementing systems, installing new hardware, and constructing the system

- infrastructure in accordance with the final design. JWA will be providing the physical network connection.
4. The Contractor shall incorporate into its project and communications plan with Airport any pertinent details regarding equipment manufacturing, procurement, tariffs, and shipping activities related to any supply chain element that could pose risk to budgets, schedules, and operations. Contractor shall coordinate as needed with the Airport to develop a mutually approved mitigation and response plan.
 5. Contractor shall organize and conduct work sessions to identify, validate, and document project requirements. These sessions shall take place thirty (30) days after notice to proceed. A minimum of ten (10) two-hour sessions is recommended. These sessions shall cover the following subjects, at a minimum:
 - a. CUPPS
 - b. CUSS
 - c. CMS
 - d. RMS
 - e. Cybersecurity/PCI DSS
 - f. Airline Specifics (e.g., phasing requirements, training, peripherals, host requirements)
 - g. Server Architecture
 - h. Cloud Connectivity
 - i. Network Architecture
 - j. Integration Architecture
 - k. Implementation Plan/Schedule
 - l. Testing and Training Requirements
 - m. JWA/County Processes (Airport Operations, Safety Training, Airport Emergency Plan, Change Management, etc.)
 - n. Disaster Recovery/Business Continuity
 6. The work sessions should include these six (6) steps:
 - a. Contractor shall identify any additional sessions required and submit the County Project Manager for approval a proposed agenda for the session, including the intended outcome, recommended list of participants, and the expected duration.
 - b. Sessions shall be conducted with, but not limited to, JWA, participating airlines, and other stakeholders as determined necessary.
 - c. All sessions shall be coordinated with the County Project Manager.
 - d. Contractor shall provide relevant expertise in guiding the sessions.
 - e. At the completion of each session, Contractor shall produce and provide to the County Project Manager a set of detailed minutes and any other appropriate documentation describing the content and outcome of the session.

- f. Record sessions, post to County project site.

B. AIRLINE APPLICATION CHANGES

1. Describe the specific application change process Contractor intends to impose on the Airport's airlines. Address each step of the process, from initial change request through deployment, for each type of change, whether it requires formal re-certification or not. Also, address expected duration and airline involvement during each process step.
2. Describe how Contractor anticipates the certification process changing over time.
3. Provide a list of all airlines currently certified on the Contractor's CUPPS and CUSS platforms, with designation of the certified platform.
4. Provide a detailed description of the Contractor's Host Connectivity Solution for airlines. Explain the process of providing this solution to airlines as well as the costs and benefits to the airlines.
5. Provide a detailed breakdown of any costs that an airline may pay directly to Contractor, beyond the licensing and support costs paid by JWA, including services provided at the Airport as well as all costs associated with application changes and certification, such as lab time, deployment, etc.

C. IMPLEMENTATION

1. Describe, in detail, the implementation approach in accordance with the requirements for project implementation.
2. The Contractor shall be responsible for the demolition and removal of unneeded existing equipment. (existing head end and other equipment).
3. The Contractor shall coordinate with the Airport on phasing of equipment implementation. (specifically phasing of gate, ticketing, and kiosk equipment) Phasing shall be conducted in a manner that limits impact to ongoing operation.
4. The Contractor shall conduct installation within the following parameters:
 - a. Standard activities can be conducted during off hours, 9pm - 5am each day (based on final Airport approval of implementation plan).
 - b. Disruptive activities (noisy, creation of odors/dust) shall be conducted from 11pm - 5am.
 - c. Work sites must be clean and ready to operations by 5am each day.
 - d. Installation shall be completed in two (2) phases at a minimum, allowing for half of each ticket lobby counter and gate counter to continue being used until the new CUPPS equipment pass all required testing and staff are trained to use the new system with an additional ten (10) business day transition time. Additionally, CUSS kiosks shall also be installed in two phases, allowing half of the units (the two (2) units closest to the entry doors) to have new kiosks installed first while the other two (2) units remain on the existing CUSS platform until the new units pass all required testing and staff are trained to use the new CUSS platform with an additional ten (10) business day transition time. All installations done pursuant to this Contract shall be routine and usual work that is incidental to the replacement of the CUPPS/CUSS equipment.
5. Describe the approach to completing the work sessions as defined in the Design Phase, along with Contractor's recommendation for what sessions should be completed.

6. Describe approach to providing quality assurance and control in accommodating the stated quality requirements.
7. Describe a high-level risk management strategy that defines Contractor's approach to identifying and mitigating project risks including, but not limited to, schedule and budget variances.
8. Provide a Work Breakdown Structure and High-Level Milestone Schedule defining the tasks required to meet the specifications for Project Implementation. Identify dependencies on activities provided by others.
9. The Contractor shall describe the high-level schedule for system implementation and provide a sample Project Plan identifying the various steps in the process and the estimated duration of each step. The plan should include airline connectivity, installation, programming, testing, and final acceptance of the new System. **(Provide as Appendix L – Proposed Implementation Schedule)**
10. In the event of a delay, and delay is the result of subcontractor performance, the Contractor shall provide all necessary overtime and additional labor as required to catch up with accepted implementation schedule.

D. PROJECT EXECUTION

1. Contractor shall provide project management and quality control services for the coordination of the Contractor and Contractor's subcontractors during the term of the Project.
2. Contractor's Project Manager and other key personnel shall support overall Project objectives and work effectively with County Project Manager, Project team and Project partners, and shall function as the liaisons between County Project Manager and the Contractor on all matters relating to the Project.
3. JWA shall approve all personnel assigned to the project. All personnel must complete a Criminal History Record Check (CHRC) and Security Threat Assessment (STA). Replacement of key personnel must be approved by JWA.
4. All Contractor personnel shall comply with JWA badging and security requirements.
5. Contractor shall provide a project manager for the duration of the project with the ability to be on-site throughout the course of the project. Final duration of onsite time will be coordinated with JWA.
6. Contractor shall conduct a project kickoff meeting, with timing coordinated with JWA. The Contractor shall present a draft project plan, project schedule, communications plan, problem escalation procedures, and introduce Contractor staff.
7. Contractor shall provide a team to deal with cutover problems or unexpected system outages that can occur at unusual hours or unexpectedly. Contractor shall submit proposed team for approval by County Project Manager.
8. Contractor, along with the County Project Manager, shall conduct regular status review meetings, as desired and agreed upon by JWA, regarding frequency, to report on scope, schedule, resources, quality, and risk mitigation.
9. The Contractor shall hold monthly stakeholder meetings, which may include JWA executives and airline representation – at the discretion of the County Project Manager.

10. Throughout design and installation, the Contractor shall provide weekly written status reports. At the discretion of JWA, a virtual meeting shall be conducted to review any emailed project status reports.
11. Contractor shall record and submit electronically a weekly summary of work throughout the project.
12. Contractor shall provide final tasks from the Project Schedule to the County Project Manager for review and approval.
13. The Project Schedule shall identify activities, scheduling, and show relationships between activities such as "develop concepts, approve initial and final concepts, completion of design documents, and completion of design" and similar milestone activities. The level of detail shall be satisfactory to JWA.
14. The Project Schedule shall begin on the day after execution of Contract Award and conclude with the date of Final Acceptance of the Project.
15. The Project Schedule shall include a ten (10) working day JWA review cycle for all deliverables.
16. Design Phase: Upon the Notice-to-Proceed, the Contractor shall begin the Design Phase, which may include Conceptual Design and Schematic Design, in coordination with JWA. The Contractor shall provide a design for the new system that shall meet or surpass the required features, functions, characteristics, qualities and/or properties within this scope of work.
17. Installation Phase: The Installation Phase is the period of the project in which the system is constructed or implemented. The Installation Phase also includes the testing, inspection, adjustment, correction and certification systems to ensure that the system performs as specified. The Installation Phase ends with Final Acceptance of the system/project.
18. Training: Before the users of the system can perform User Acceptance Training (UAT), training must be provided. Training shall involve the training of both User training and Maintenance training (airline training). It is preferred that the Contractor provide the following services:
 - a. Testing Phase: Prior to the Production, the Contractor shall perform, the following test phases at minimum.
 - i. Factor Acceptance Testing: These tests shall include the testing of all the peripherals with the system, to confirm that they meet the Technical Requirements.
 - ii. Integration Testing: Integration testing shall be performed to verify combined functionality after integration with other systems. The testing should verify that the individual components are communicating, both in terms of protocol and content, with each other, as required.
 - iii. User Acceptance Testing (UAT): UAT shall validate that the system is performing as expected. User Acceptance shall not be completed until all phases of the system installation have been successfully completed and tested. All User Acceptance Testing shall be completed prior to production Go-Live.
 - iv. Endurance Testing: Endurance testing shall demonstrate that the systems perform in the production environment without downtime caused by system errors for a minimum duration of 30 calendar days. Any major issues or downtime will require restart of the endurance testing.

- v. Final System Acceptance: Final System Acceptance shall not occur until UAT Testing and all phases of the installation have been successfully completed and approved by JWA.
19. Rollout Production Go-Live: In coordination with UAT and with substantial completion of the training, the system shall be rolled out in production environment and shall “Go-Live.”
 - The rollout into Production and Go-Live shall be implemented according to the agreed upon Project Plan.
 - The Contractor must provide, at a minimum, on-site staff for the duration of the rollout period from Go-Live to support JWA staff in the roll out.
 20. The existing operations shall be maintained. Installation of the System shall not hinder the airline and airport operations. (Other than planned interruptions due to phasing in of new equipment)
 21. The Contractor must comply with the County’s Utility and Location Shutdown Requirements at all times - see **Exhibit A - JWA Standards Package**.
- E. TRAINING - The Contractor shall provide training for County identified and airline identified personnel in all aspects of the systems. Before the users of the system can perform User Acceptance Testing, training must be provided. Training shall involve the training for both User training and Maintenance training.
1. Develop and provide a documented Training Plan for acceptance by County staff thirty (30) days prior to the scheduled training initiation date. The Training Plan must describe the methods, techniques, course outlines, materials, syllabus, and course descriptions.
 2. Offer training for the County system administrator and users to allow input/editing of data, management of data, management of the system database, normal use and maintenance of the system, preparation for reports, and system customization.
 3. Provide hands-on training for JWA and airline personnel for the operation and maintenance of the System. Note: some resources work in alternate working shifts (i.e., 2nd or 3rd shift), the training plan should accommodate these additional shifts and stagger the days available to maximize staff attendance.
 4. Provide Standard Operating Procedures, training manuals, or job aides to each participant at the time the course is conducted.
 5. Provide all materials (except instruction manuals) delivered electronically in editable and “fixed” formats (e.g., PDF and Microsoft Office document formats)
 6. Provide updated training after each major system upgrade or release.
 7. Each course shall require JWA’s approval prior to presentation. Training shall be conducted with selected JWA personnel and end user airline personnel.
 8. At a minimum, the Contractor shall provide training on admin support, end users, troubleshooting, and all system modules. This Training should include input/editing of data, management of the system database, creation of reports, and any system customization.
 9. At a minimum, the Contractor shall provide training sessions to trusted JWA agents, such as personnel from Airport Operations, Public Affairs, IT, Sheriff’s Department, airlines, Orange County Fire Authority (OCFA), Transportation Security Agency (TSA), Customs Border Patrol (CBP), and Maintenance.

10. Contractor shall prepare and supply training materials and conduct training for all users of the Project. A master set of the training course materials; both hard copy and electronic copy shall be developed for future presentation and training purposes and distributed to JWA. The master set shall be maintained and updated with each upgrade of the system up to the conclusion of the warranty period. The sessions shall be video recorded, or the Contractor shall provide video-based, pre-recorded training for use by staff.
11. Any video-based training materials shall be computer screen recorded, not live instruction recorded.
12. Training instruction manuals shall be provided which include images (as needed) and are specific to the application proposed at JWA.
13. The following general training guidelines shall be adhered to and are considered minimum requirements:
 - a. Training courses shall be augmented by individual instruction as necessary to fully train the JWA designated resources sufficient for a complete understanding of the system and ability to troubleshoot system errors.
 - b. Training courses shall be augmented by individual instruction as necessary to fully train the Airline personnel.
 - c. Contractor shall be required to provide all training aids (e.g., notebooks, manuals, cheat sheets, reference guides, etc.).
 - d. Training shall be completed a minimum of two (2) weeks prior to the system becoming operational and utilized by airlines. Training schedule shall be subject to the JWA Project Manager's approval.
 - e. Training shall be conducted onsite at the Airport in the Airport-approved training location.
 - f. Scheduling
14. Scheduling includes:
 - a. Contractor shall develop a training schedule, working with the airlines and JWA to maximize the availability of attendees and minimize disruption to normal airline/Airport operations.
 - b. Training sessions shall be scheduled with the JWA Project Manager.
 - c. A formal training schedule shall be developed and published to JWA and airlines with the following information:
 - i. Course name
 - ii. Date and time
 - iii. Course duration
 - iv. Location
 - v. Comments on any prerequisite or preparatory tasks
15. The Contractor shall describe how training will be provided to JWA. (Training costs shall be provided in Pricing Proposal)

16. The Contractor shall provide a sample Training Plan for reference. **(Provide as Appendix M – Sample Training Plan)**

F. TESTING PLAN

1. Contractor shall develop a Master Test Plan (MTP) for each system in the procurement package. Each system should be tested, then integrations between the new systems tested, and finally integrations between new and existing systems shall be tested. This should all be outlined clearly in the MTP.
2. Contractor shall and submit the Master Test Plan (MTP) to the JWA Project Manager thirty (30) days prior to the start of testing. The MTP provides the framework for all testing necessary to be conducted according to the requirements specified.
3. The Contractor shall ensure that all system components, interfaces, and systems have successfully completed expected test parameters and have proven operationally to meet these requirements. The Test Plan should include the following, as a minimum:
 - a. Test Plan Overview
 - b. Test Plan Strategy
 - c. Testing schedule (include pre-implementation, cutover, and post implementation).
 - d. List of expected tests to be conducted
 - e. Test Cases with detailed steps
 - f. Requirements Traceability Matrix
 - g. Test Summary Reports and Defect Tracking
 - h. Requirements for each phase of testing
 - i. Test execution evidence (as requested by JWA)
4. The Contractor shall provide costing information for all testing provided. (Testing costs shall be provided in Pricing Proposal)
5. The Contractor shall provide a sample Testing Plan for reference. **(Provide as Appendix N – Sample Testing Plan)**

G. FACTORY ACCEPTANCE TESTING (FAT)

1. Contractor shall accommodate needed staff from JWA/County (or designated representatives) to come onsite to the Vendor's "factory" to do initial acceptance testing before shipping products to JWA.
2. The Factory Acceptance Testing shall include:
 - a. Test plan and script for core criteria, created by Contractor, and submitted to JWA for review and approval
 - b. Documentation of results
 - c. Remediation of any failures found during testing and retesting of the system from the beginning.
 - d. Review and acceptance by County Project Manager and Airport IT Manager.

- e. JWA reserves the right to require a complete retest of the FAT if critical issues arise during the testing.

H. USER ACCEPTANCE TESTING (UAT)

1. The Contractor shall setup mockup workstations, kiosks, and digital displays in the JWA environment, at an airport-approved testing location.
2. User Acceptance Testing shall verify the system meets each airline's user requirements as designed by the Contractor. Tests shall be conducted on systems as these systems are installed per the Contractor's Phasing Plan and Project Schedule
3. The Contractor shall supply JWA with a test plan that will be followed, including a test schedule, to execute UAT with JWA and airline representatives. The County Project Manager will be required to acknowledge acceptance and approval of the plan prior to execution. Duration of testing shall be agreed upon by JWA and Contractor. Upon successful completion of each phase of the User Acceptance Testing, the installed system(s) shall be ready for use by the Stakeholders.
4. All User Acceptance Tests will be conducted at the production Airport-approved testing location. Tests shall be scheduled with JWA at least two (2) weeks in advance.
5. UAT should not be performed until formal training has been provided to the proper Airport and project stakeholders.
6. Upon completion of Factory Acceptance testing, functional testing shall occur with Airport and project stakeholders
7. UAT shall verify that the installed system meets all the required functionality as specified in this RFP. All requirements must be cross-referenced in the UAT test plan with the appropriate UAT test script and correlating requirement in the RFP.
8. UAT must include the following:
 - a. Configured Functionalities: The test scripts must include a checklist of functional items to be verified by users for each system module. All test scripts must state intended results.
 - b. Integration Testing: The testing should verify that the individual components and systems are communicating, both in terms of protocol and content, with each other, as required.
 - c. Execution of standard, custom, and ad-hoc reports.
 - d. Testing of Cybersecurity controls thru Internal and External penetration and vulnerability scans.
 - e. Final UAT testing shall be conducted in the production environment prior to actually going live.
 - f. Any discrepancies, errors, or issues discovered during these tests shall be logged and corrected by the Contractor at no cost to JWA.
9. UAT shall be conducted as part of the Phasing Plan and shall need to be accepted by JWA prior to going live for each phase of installation in accordance with the Installation Schedule and Phasing Plan.
10. UAT shall be conducted in accordance with the approved User Acceptance Test plan developed by the Contractor and agreed to by JWA staff.

11. The Contractor shall develop UAT test plans, including test scripts and procedures to test every component, function, feature, and integration of the system.
12. The UAT test plan must be submitted for review and approval by JWA. Once reviewed and approval has been received by JWA, testing may be performed.
13. The UAT test plan shall designate what constitutes high, medium, and low priority defects and resolution requirements for each.
14. Fix and retest duration shall not exceed ten (10) business days.
15. Upon completion of the UAT, the Contractor shall seek formal signoff and signatures from JWA to approve UAT completion. Formal signoff and signatures can include email acceptance and signoff, screenshots and/or hardcopy documentation, to show test results and acceptance of the system.
16. Throughout the testing phase, Contractor shall provide regular updates on overall testing progress and results. The Contractor Project Manager shall gather and provide all necessary documentation for evidence of acceptance from project stakeholders.
17. The Contractor shall provide a failover test of all equipment during the testing period.

I. ENDURANCE TESTING

1. The FAT and UAT must be completed and approved prior to commencement of Endurance Testing.
2. The Contractor shall submit an Endurance Plan for review and approval by JWA, which includes success criteria, issues resolution plan, and other details coordinated with the County Project Manager.
3. System endurance testing shall run for a period of sixty (60) days past Go-Live of that system. The sixty (60) days shall be divided into an initial thirty (30) days for first phase of implementation (subject to final implementation plan) and final thirty (30) days. For the CUPPS gate positions, endurance will start on each gate's Go-Live. The Contractor shall make no adjustments or changes to the system, unless approved by the County Project Manager, during this period.
4. The Endurance Test shall include a failover test at the end of each phase, as coordinated with JWA.
5. Endurance testing shall ensure the system, as implemented, is stable and can perform without any issues over a sustained period.
6. The system shall perform as expected and meet all requirements included in this scope of work for thirty (30) consecutive days without any performance or availability issues.
7. The Contractor shall keep track of all issues that arise during this phase of endurance testing.
8. The Contractor shall work with JWA to develop the criteria for major and minor issues. Major issues shall include any issues that arise which impact the overall stability, availability, data integrity, or performance of the system.
9. The endurance testing period shall restart in entirety for any major issues (shall include any issues that arise that impact the overall stability, availability, data integrity, or performance of the systems) found during this period and shall require the Contractor to correct the issues and reset the thirty (30) day endurance period.

10. Upon successful completion of endurance testing, the Contractor shall seek formal signoff and signatures from JWA to approve completion of the endurance testing.

J. FINAL SYSTEM ACCEPTANCE

1. At the completion of the Endurance Testing period, the County Project Manager shall review and approve the system implementation completion. If not approved, the County Project Manager will work with the Contractor to adjust any final items.
2. Final acceptance of the system can only occur with the successful completion of the thirty (30) day endurance test.
3. Final acceptance shall not occur until all phases of installation have been successfully performed and the thirty (30) day endurance period has been completed and approved by JWA.
4. Only upon formal acceptance of endurance testing, the Contractor and system can move into the warranty phase of the project.
5. The Contractor shall seek formal acceptance of the system only upon the successful completion of endurance testing. JWA shall provide a certificate of final acceptance once all conditions above have been met.
6. Final Acceptance shall be withheld until the following activities have been successfully completed:
 - a. Formal acceptance of Endurance Testing
 - b. Approval of all submittals
 - c. Delivery of final documentation and materials (as-builts, warranties, O&M manuals, signed permit cards, IP address tables, hardware & software user accounts, passwords, locations, support contracts, configurations, asset inventory lists, etc.)
 - d. Provide County with evidence required to receive Successful Report of Compliance from PCI or provide County with certification of compliance from PCI.

22. WARRANTY REQUIREMENTS

A. GENERAL WARRANTY

1. The Contractor shall provide warranty services for the entire system during the installation and for an additional twelve (12) months after Final System Acceptance. This warranty shall cover all new equipment and software provided as part of this scope. All software and firmware provided as a part of the project, including major and minor releases, shall be upgradeable, for the purpose of improving functionality or debugging, and without cost to JWA, during the Warranty period.
2. The Contractor shall transfer all original equipment manufacturers' hardware warranties to JWA upon system commissioning.
3. The Contractor shall provide a list of required spare parts inventory and shall furnish each inventory of spare parts (type, model number, and quantity) during the warranty period. Required spares shall be on-site at the time of final system acceptance. To ensure service levels can be met, during the Warranty Period, the Contractor shall maintain an adequate inventory of spare parts of all hardware provided by the Contractor. At its sole expense, Contractor shall immediately replenish such inventory whenever parts are removed.

4. Spare parts shall be new and not refurbished or repaired parts. Defective parts and parts that fail prior to project completion, purchased for this project, shall be replaced with new parts, not sent away for repair, and reinserted into the project as spare parts inventory and operational use.
5. During the Warranty period, all costs to maintain the system shall be fully burdened by the Contractor. Including all consumables and, software/firmware updates. Costing for consumables in particular should be identified in Pricing Proposal. For consumables, JWA reserves the right to purchase internally if the cost does not meet expectations.
6. The Contractor shall provide a sample Warranty for JWA to review. **(Provide as Appendix O – Warranty Plan)**
7. If JWA detects an issue with the installed system during the Warranty period, the Contractor shall, at no additional cost, provide a fix in a timely manner (resolution starting within forty-eight (48) hours of notification from JWA). JWA will notify the Contractor through email or phone call to the appropriate contact. The Contractor shall describe the methodology for fixing issues during a Warranty period.
8. The Contractor shall test, install, and train end users (if appropriate) on all minor and major system upgrades during the Warranty period. Upgrade plans, including testing procedures, scheduling of activities, and objectives will be approved by JWA. Approved upgrades shall be installed within three (3) months of release date, or as agreed to by the Airline
9. All 3rd party software licenses shall be purchased by the Contractor in the name of the Airport. The Contractor shall inform JWA if this cannot be completed.
10. After the twelve (12) month Warranty period, the Contractor immediately transitions into the Maintenance and Support period.

23. MAINTENANCE AND SUPPORT REQUIREMENTS

A. CHANGE MANAGEMENT

1. The Contractor will document all systems changes to production systems and provide a formal change request to JWA no less than three (3) business days in advance prior to execution of the change. This documentation shall meet the current PCI DSS v4.0.1 or most current standard at the time of contract award (which includes documenting impacts are outlined per change). For emergency changes vendor shall submit a change request as soon as practicable. Upon completion of each change Contractor shall provide evidence of completion for JWA's review and final approval.

B. MAINTENANCE

1. The Contractor shall provide a maintenance plan and describe methods for correcting issues arising with the system.
2. The Contractor shall provide upgrades and recurring monthly patching for maintenance of the system. The Contractor shall provide a plan describing how this will be accomplished.
3. The Contractor shall provide the contact information of staff responsible for resolving major issues with the system. This shall include a toll-free line and other contact information as deemed appropriate by the Contractor.
4. The Contractor shall test and install all software and firmware upgrades for the purpose of improving functionality or debugging. The Contractor shall advise JWA of the availability of

- any Major Release that it or its licensors offer to any of their customers and provide JWA with all information and assistance necessary to enable JWA to determine whether or not to implement the Major Releases.
5. The Contractor shall ensure that the installation of any minor or major system upgrade is capable of being immediately reversed. If the upgrade provokes difficulties, the Contractor shall at its expense resolve any such difficulty, including by reversing such installation, or at JWA's request immediately reversing such installation.
 6. The Contractor shall continue to provide certified airline applications modifications and upgrades for all airlines operating on the CUPPS at JWA, including any new airlines that begin operations after the Warranty Period.
 7. JWA will negotiate the length of the Maintenance period with the selected Contractor.

C. SUPPORT

1. The Contractor shall provide all support through one service provider (including having one entity to call for any support needs). Even if the Contractor uses a subcontractor or partner in supplying elements of the proposal, all support shall be managed by the Contractor.
2. The Contractor shall be required to provide support for the system. As a minimum, the following shall be provided:
 - a. 24/7 Availability
 - b. 24/7 US-based agent call center that will receive all end-user, County trusted agent calls and dispatch Level 1 service calls to County, Level 2-3 will be escalated to Contractor's own support staff.
 - c. Call center shall provide an agent-based call queue system capable of reporting at a minimum, number of calls in queue, longest and average wait times, number of dropped calls, and calls taken per agent.
 - d. Support staff onsite from 8am – 4pm, seven (7) days a week (assuming approximately 2.5 Full Time Employee (FTE) for the duration of the contract).
 - e. On-call support staff between 4pm - 8pm, seven (7) days a week will be able to respond within a reasonable timeframe (return any missed call within thirty (30) minutes, be on-site, if necessary, within one (1) hour).
 - f. Support staff shall be available during any ad hoc or regularly scheduled maintenance, with twenty-four (24) hours advance notice, to perform system testing and validation.
 - g. Use of JWA provided office space for onsite staff.
 - h. Describe your support model that will support the County's level of service.
 - i. Refer to SLR for complete Service Requirements **Attachment D - JWA SLR Requirements.**
3. JWA will provide first-level support services (onsite/break-fix of non-proprietary Contractor hardware) for coverage and performance suitable to the number of systems.
4. The Contractor shall describe in detail how the proposed plan would meet JWA's needs and the needs of its stakeholders, based on current flight schedules and operations from airports of similar size and operating models

5. The following list provides the current level 2 and 3 support activities performed by the common use provider. The Contractor shall provide these at a minimum:
 - a. Contractor's on-site interface to JWA, reporting duties to Contractor HQ.
 - b. Provide direction to JWA's local Support Team in delivering service to the end user.
 - c. Site Administrator will recommend spare management. Spares will be purchased by Contractor under Task Order budget with JWA or JWA direct purchase.
 - d. Site Administrator will be the airline and JWA's main point of contact and first escalation point for the function topics as defined in this list of job functions.
 - e. Ensuring shortest possible restore times escalations to Contractor specialized resolver groups, when necessary.
 - f. Communicating with the airlines and JWA to understand business and technical requirements.
 - g. Maintain accurate records pertaining to the inventory and all relevant account documentation.
 - h. Resolve complaints and prevent recurrence of repetitive issues.
 - i. Extensive product knowledge of airline systems and common use systems.
 - j. Regular meetings with airline station managers to discuss common use projects.
 - k. Regularly monitor status, health and performance of the common use servers, ensure applicable updates and security patching is performed.
 - l. Check and validate any alerts received from Contractor monitoring system and ensure findings are reported back to Contractor for support, as required.
 - m. Network testing to the Airport demarcation point, when required, for fault finding for common use workstations.
 - n. Determine source of network issues (local or host).
 - o. Triage network configuration issues with both airline IT and JWA IT.
 - p. Perform Disaster Recovery monitoring and execution, as required.
 - q. Pro-active monitoring of all systems to discover any issues that might have negative impact on service and infrastructure operations.
 - r. Following common use workstation setup plans, maintain commonality throughout the common use environment.
 - s. Assist with implementation of new airlines, agents and airline applications on the common use system and updates for existing airlines, when needed.
 - t. Provide assistance in setting up workstations or replacing on the common use platform.
 - u. Update, add and remove common use certified airlines and required peripherals on the common use platform.
 - v. Assist various support levels with fault-finding activities for airline systems when reported.

- w. Act as hands and feet for remote support and service engineers, as necessary.
 - x. Provide supporting role in JWA change management process, as necessary.
 - y. Conduct required diagnostics and report and escalate technical problems, which cannot be readily resolved and track through to resolution.
 - z. Provide support for power outages, either scheduled or non-scheduled, as required.
 - aa. Provide support for common use platform maintenance, either scheduled or non-scheduled, as required.
 - bb. Regular and ongoing onsite equipment repair for peripheral equipment devices to maintain adequate and recommended “working” spare quantity.
 - cc. Process CMS and RMS changes and implement images.
 - dd. Provide support and lead cybersecurity program and compliance efforts for all components within the CUPPS at the direction of County’s IT Security Manager.
 - ee. Respond to security incidents, provide reporting to County and other stakeholders, lead and support efforts during the identification, containment, eradication, recovery, and post incident analysis of all common use systems.
6. The County currently provides the following level 1 support activities:
- a. Contractor Site Admin will address any resource concerns with common use Sr. Technologist or IT Manager.
 - b. Expected to address common use system or user incidents as a first priority (i.e. a higher priority than any other JWA assigned tasks) as determined by JWA Management. County IT leadership will set priorities based on severity, business impact, etc.
 - c. Are first responders when on-site response required as directed by the Contractor Service Desk personnel.
 - d. Will provide timely responses to the Service Desk through email to document when an incident ticket is acknowledged and resolved.
 - e. Responsible for escalating incidents to the Site Admin through the Service Desk by routing incident tickets to L2 Site Admin support.
 - f. Responsible for providing feedback to users on fault resolution
 - g. Responsible for initial resolution of user issues such as log in, program access, peripheral access, replacement of defective peripheral hardware.
 - h. Responsible for delivering Planned Hardware Maintenance schedule recommended by the Site Admin, who is responsible for escalation and coordinating resources from other third-party suppliers (i.e., OCIT/SAIC).
7. The Contractor shall describe the support escalation process for both Airport and airline staff.
8. The Contractor shall service and support the software to ensure that the software continues to operate in accordance with the intended purposes and industry best practices. This includes the prompt provision by the Contractor of the following services:
- a. Informing JWA of any defects or errors in the software that it becomes aware of.

- b. Correcting any defect or error in the software through the procedures established in coordination with County Project Manager.
 - c. Addressing any functional failures between the airlines' applications and the CUPPS software.
 - d. Addressing any functional failures between the airlines' applications and the CUSS software.
 - e. Perform root cause analysis when required.
9. All support related costs shall be included in Pricing Proposal.
 10. The Contractor shall describe the required support to be provided by the Airport for the system to be maintained.
 11. The Contractor shall maintain the CUPPS platform in a manner capable of supporting successful PCI compliance.

D. VUNERABILITY MANAGEMENT

1. County shall conduct recurring monthly vulnerability scans against Contractor's environment.
2. Contractor shall remediate any vulnerabilities identified as high or critical within thirty (30) days during the next monthly patching cycle.
3. Contractor shall remediate any vulnerabilities the County identifies as urgent as soon as practical as mutually agreed upon with JWA. Contractor shall coordinate with JWA within forty-eight (48) hours of notification of any urgent vulnerabilities.
4. For any updated or vulnerabilities that cannot be remediated, Contractor shall advise JWA on mitigation strategies in accordance with the County risk variance process. JWA is responsible for approving all variances.

E. MONTHLY REPORTING

1. Contractor shall hold a recurring service review meeting with JWA. The meeting cadence shall be coordinated with County IT Project Manager.
2. Contractor shall provide monthly report by the seventh (7th) day of the following month covering at a minimum, call center agent and queue metrics, monthly service and incident tickets, system uptime availability, recurring maintenance and change requests, and usage statistics for CUPPS and CUSS.

F. SERVICE LEVEL AGREEMENT

1. The Contractor shall provide systems with a Service Level Requirement (SLR) to ensure a high level of availability (99.999%) with downtime for maintenance and testing not included.
2. The Contractor shall provide SLRs that meet or exceed expectations as outlined in **Attachment D - JWA SLR Requirements.**
3. The Contractor shall include all SLR terms and conditions.
4. County reserves the right to impose invoice deductions if the SLRs are not met.
5. Refer to the SLR expectations as outlined in **Attachment D - JWA SLR Requirements.**

6. Describe the proposed SLR's for the solution set and how those would vary depending on whether the final solution was totally cloud based, totally On-Premise, or a hybrid solution.
7. The Contractor shall coordinate with JWA to finalize a mutually approved service model and staffing plan.

24. OPTIONAL SCOPE

- A. Local Departure Control System (LDCS) REQUIREMENTS - JWA is considering the addition of an LDCS. The following requirements are specifically for LDCS.
 1. The Contractor shall describe the licensing agreement for the LDCS application that is consistent with the initial capacity and expansion capability requirements.
 2. The Contractor shall list the system application software modules including:
 - a. A description of the functionality being offered.
 - b. Current application software version.
 - c. When the current software version was released.
 - d. When the next version is planned.
 3. The Contractor shall specify if the LDCS is a standalone application or is offered as an integrated module of the CUPPS platform. Include discussion on if the LDCS is provided by the Contractor or a third party.
 4. Contractor shall describe how the LDCS accommodates aircraft of different sizes and configurations (e.g., graphical management of cabin plans).
 5. Contractor shall describe how the LDCS supports import of flight and passenger data. Include discussion on the type of messaging and formats available.
 6. Contractor shall describe how the LDCS supports IATA standard boarding passes and baggage tags.
 7. Contractor shall describe if the LDCS notifies agents to collect excess baggage charges (if applicable).
 8. Contractor shall describe how the LDCS supports generation of load sheets.
 9. Contractor shall describe how the LDCS accommodates Baggage Source Messages (BSMs) for the Baggage Handling System (BHS).
 10. Contractor shall describe how the LDCS accommodates moving baggage to makeup areas without a BSM to enhance system redundancy.
 11. Contractor shall provide costing for the LDCS in Pricing Proposal.

25. INNOVATION ROADMAP

The Airport is looking for a technology partner and wishes to review innovative options that the proposing Contractor has to offer. There will be twenty-five (25) points allotted for Efficiencies and Innovation in the Effectiveness of Project Approach Methodology Evaluation Criteria. All costs for the following items shall be included in Pricing Proposal. If the Contractor should include details on if they are able to provide the following innovations and options:

A. SELF BAG DROP

1. The Contractor shall describe how its common use self-service bag drop solution set could help the Airport accomplish its business objectives of providing a more seamless passenger journey.
2. The Contractor shall include the following, at a minimum:
 - a. A high-level system architecture diagram indicating major components and connectivity to LAN, airline DCS's, and other Passenger Processing, Baggage and Operational systems.
 - b. A narrative describing core and optional features of the bag drop solution set that could be advantageous given the passenger and airline mix of airports similar to JWA.
 - c. A description of the process by which the Contractor would help JWA analyze business operations of and provide recommendations for One-Step, Two-Step, or Hybrid Models of Bag Drop technology.
 - d. A description of the interfaces required, e.g. Baggage Source Message (BSM) Broker, airline DCS, CUPPS/CUSS, Airport Operational Database (AODB), FIDS, RMS, and BHS, and what type(s) of integration technologies JWA would need to provide for operational success.
 - e. A review of the current airline mix at JWA and an assessment of each airline's application level of readiness for self-service bag drop.
 - f. Optional unit pricing for self-service bag drop technology as noted in the Pricing Proposal.

B. BHS INTEGRATIONS

1. The Contractor shall describe BHS integrations (such as BSM and Baggage Reconciliation System (BRS) support) that are available for the Airport in the future. The Contractor shall describe the implementation of these integrations at other airports.

C. BIOMETRICS

1. The Contractor shall describe what biometric integrations are available in the CUPPS solution.
2. The Contractor shall describe the ability to provide a biometric exit solution at the gates.

D. MOBILE OPTIONS

1. The Contractor shall explain any mobile options available for the system (e.g., tables for roaming agents or the use of mobile carts). Additionally, the Contractor shall explain what the connectivity requirements are for these options (cellular/Wi-Fi).

E. RMS INTEGRATIONS

1. The Contractor shall describe possible RMS financial modules and integrations.

26. ATTACHMENTS, APPENDICES AND EXHIBITS

These Appendices will be provided by Contractor using the following naming convention:

- A. Appendix A - CUPPS Architecture Diagram
- B. Appendix B - CUSS Architecture Diagram

- C. Appendix C - CMS Architecture Diagram
- D. Appendix D - RMS Architecture Diagram
- E. Appendix E - CUPPS Configuration Diagram
- F. Appendix F - CUPPS Millwork Diagram
- G. Appendix G - CUSS Kiosk Diagram
- H. Appendix H - CMS Display Diagram
- I. Appendix I - CUPPS Interface Diagram
- J. Appendix J - CMS Interface Diagram
- K. Appendix K - RMS Interface Diagram
- L. Appendix L - Proposed Implementation Schedule
- M. Appendix M - Sample Training Plan
- N. Appendix N - Sample Testing Plan
- O. Appendix O - Warranty Plan

Attachments and Exhibits are provided documents for Contractor reference and may become part of the Contract.

27. ADDITIONAL WORK CLAUSE FOR APPLICABLE SERVICE CONTRACTS:

- A. Upon County request, Contractor shall submit supplemental proposals for Additional Work not called for under the Scope of Work of this Contract. Contractor must obtain County Project Manager's written approval prior to commencing any additional work.
- B. County reserves the right to obtain supplemental proposals from, and use, alternate sources for completion of the additional work and to utilize the data provided under this Contract to obtain necessary services.
- C. If County authorizes work by an alternate source, Contractor may be relieved of responsibilities pertaining to the equipment affected by the project while work is being performed and during the subsequent warranty period.
- D. Contractor shall continue to provide services to all areas not affected by work provided by alternate sources.
- E. Upon completion of any additional work, whether by Contractor or an alternative source, County's Project Manager or designee and Contractor will inspect the finished product at no additional cost to County. Upon mutual acceptance of the additional work, Contractor shall again be responsible for all services originally covered under this Contract and the work performed under this section.

ATTACHMENT B
PAYMENT/COMPENSATION

1. **Compensation:** This is a firm fixed fee Contract between County and Contractor for Service Description as set forth in Attachment A, "Scope of Work".

Contractor agrees to accept the specified compensation as set forth in this Contract as full payment for performing all services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until acceptance, for risks connected with the services, and for performance by Contractor of all its duties and obligations hereunder. Contractor shall only be compensated as set forth herein for work performed in accordance with the Scope of Work. **County shall have no obligation to pay any sum in excess of the fixed rates specified herein unless authorized by amendment in accordance with Articles "Changes" and "Amendments" of County Contract Terms and Conditions, which may require approval by the County Board of Supervisors.**

2. **Fees and Charges:** County will pay the following fees in accordance with the provisions of this Contract. Payment shall be as follows:

TBD Upon Contract Award

Additional Work: Any additional services not listed in the Contract must be approved by County's Project Manager or designee in accordance with Attachment "A", Scope of Work, Item #27.

Additional work shall not exceed per year: TBD

Total Contract amount not to exceed: TBD

3. **Price Increase/Decreases:** No price increases will be considered during the first term of the Contract. County requires documented proof of cost increases on Contracts prior to any price adjustment. A minimum of 30-days advance notice in writing is required for consideration of such adjustment. No retroactive price adjustments will be considered. All price decreases will automatically be extended to County of Orange. County may enforce, negotiate, or cancel escalating price Contracts or take any other action it deems appropriate, as it sees fit. The net dollar amount of profit will remain firm during the period of Contract. Adjustments increasing Contractor's profit will not be allowed.
4. **Firm Discount and Pricing Structure:** Contractor guarantees that prices quoted are equal to or less than prices quoted to any other local, State or Federal government entity for services of equal or lesser scope. Contractor agrees that no price increases shall be passed along to County during the term of this Contract not otherwise specified and provided for within this Contract.
5. **Contractor's Expense:** Contractor will be responsible for all costs related to photo copying, telephone communications and fax communications while on County sites during the performance of work and services under this Contract.
6. **Final Payment:** Final payment shall be issued based on the completion of the work as described in this Contract and County Project Manager accepts all the work and JWA issued badges are returned to Badging Office.
7. **Payment Terms – Payment in Arrears:** Invoices are to be submitted in arrears to the user agency/department to the ship-to address, unless otherwise directed in this Contract. Contractor shall reference Contract number on invoice. Payment will be net thirty (30) days after receipt of an invoice in a format acceptable to County of Orange and verified and approved by the agency/department and subject to routine processing requirements. The responsibility for providing an acceptable invoice rests with Contractor.

Billing shall cover services and/or goods not previously invoiced. Contractor shall reimburse County of Orange for any monies paid to Contractor for goods or services not provided or when goods or services do not meet Contract requirements.

Payments made by the County shall not preclude the right of the County from thereafter disputing any items or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.

8. **Payment – Invoicing Instructions:** The Contractor will provide an invoice on the Contractor's letterhead for goods delivered and/or services rendered. In the case of goods, the Contractor will leave an invoice with each delivery. Each invoice will have a number and will include the following information:
 - A. Contractor's name and address
 - B. Contractor's remittance address, if different from 1 above
 - C. Contractor's Federal Taxpayer ID Number
 - D. Name of County Agency/Department
 - E. Delivery/service address
 - F. Master Agreement (MA) or Purchase Order (PO) number
 - G. Agency/Department's Account Number
 - H. Date of invoice and invoice number

- I. Product/service description, quantity, and prices
- J. Order Date/Service Date(s)
- K. Sales tax, if applicable
- L. Freight/delivery charges, if applicable
- M. Total

Invoices and support documentation are to be forwarded to **(not both)**:

Mailed to John Wayne Airport
 Attention: Accounts Payable
 3160 Airway Avenue
 Costa Mesa, CA 92626

OR

Emailed to AccountsPayable@ocair.com

9. **Payment (Electronic Funds Transfer (EFT)):**

County of Orange offers contractors the option of receiving payment directly to their bank account via an Electronic Fund Transfer (EFT) process in lieu of a check payment. Payment made via EFT will also receive an Electronic Remittance Advice with the payment details via e-mail. An e-mail address will need to be provided to The County of Orange via an EFT Authorization Form. To request a form, please contact the agency/department Procurement Buyer listed in Contract. Upon completion of the form, please mail, fax or email to the address or phone listed on the form.