AMENDMENT NUMBER TWO FOR COMMON-USE PASSENGER PROCESSING SYSTEM, "CUPPS" MAINTENANCE AND REPAIR

This Amendment 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, through its department John Wayne Airport ("County" or "JWA") and SITA IPS USA Corp. ("Contractor"), with County and Contractor sometimes individually referred to as "Party" or collectively referred to as "Parties."

RECITALS

WHEREAS, County and Materna IPS USA Corp. entered into Contract MA-280-20011231 for Common-Use Passenger Processing System, "CUPPS" Maintenance and Repair, effective June 1, 2020, through May 31, 2023, with a Total Contract Amount Not to Exceed $6,386,780.00 ("Contract"); and,

WHEREAS, pursuant to Amendment Number One, County and Materna IPS USA Corp. renewed the Contract for two additional (2) years, effective June 1, 2023, through May 31, 2025, and amended various Attachments and Contract provisions, with a new Total Contract Amount Not to Exceed $5,075,801.00; and,

WHEREAS, on December 12, 2024, as a result of an acquisition by Contractor, an Assignment, Novation and Consent Agreement was executed to transfer and assign the Contract from "Materna IPS USA Corp." to Contractor, effective as of October 11, 2024; and

WHEREAS, the Parties now desire to extend the Contract for two additional (2) years, effective June 1, 2025 through May 31, 2027, with a Total Contract Amount Not to Exceed $3,535,795.88, revise Attachment G, Fees and Charges; replace Attachments A and D, and amend various Contract provisions to reflect revised County policies and update the Parties' notice Information; and,

NOW, THEREFORE, in consideration of the mutual obligations set forth herein, the Parties agree as follows:

AMENDMENT TO CONTRACT ARTICLES

1. Section 2 of the Contract's Additional Terms and Conditions shall be amended to read in its entirety as follows:

   2. **Term of Contract:** The Contract shall be extended, commencing June 1, 2025, and shall be effective for two (2) years, unless otherwise terminated as provided herein.

2. Section 3 of the Contract's Additional Terms and Conditions shall be amended to read in its entirety as follows:

   3. **Contract Amount Not to Exceed:** Contract Amount Not to Exceed $3,535,795.88.

3. Attachment A, Scope of Work is amended in its entirety as attached hereto.

4. Attachment D, Subcontractors is amended in its entirety as attached hereto.

5. Attachment G, Fees & Charges is revised in its entirety as attached hereto.

6. Section T. of the Contract's General Terms and Conditions shall be amended to read in its entirety as follows:

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.

7. Section 13 of the Contract's Additional Terms and Conditions shall be amended to read in its entirety as follows:

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 County. This obligation shall apply to Contractor, 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 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.

8. Section 57 of the Contract's Additional Terms and Conditions shall be amendment to read in its entirety as follows:

57. **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.

9. Section 37, Notices of the Contract's Additional Terms and Conditions shall be amended to read in its entirety as follows:

37. **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 Deputy Purchasing Agent (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:
SITA IPS USA Corp.
Attn: Daniel Dunn, Senior Manager Infrastructure Management
5323 Millenia Lakes Blvd Ste 300
Orlando, FL 32839
Phone: (941) 928-0046
Email: Daniel.Dunn@sita.aero

Cc:
SITA IPS USA Corp.
Attn: Contracts Management
600 Galleria Parkway SE, Suite 1000
Atlanta, GA 303339
Email: amer.contract.management@sita.aero

County's Project Manager:
JWA/Innovation & Technology
Attn: William Bogdan, Project Manager
3160 Airway Avenue
Costa Mesa, CA 92626
Phone: (949) 255-1336
Email: wbogdan@ocair.com

cc: JWA/Procurement
Attn: Monica Rodriguez, County DPA
3160 Airway Avenue
Costa Mesa, CA 92626
Phone: (949) 252-5175
Email: mrodriguez@ocair.com

10. All other terms and conditions in this Contract, except as specifically amended herein, shall remain unchanged and with full force and effect.

(*signature page follows*)

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment on the date first above written.

SITA IPS USA Corp*

Signiert von:
Georg Oschmann
6C73209FA265486...
Georg Oschmann CEO SITA IPS 4/8/2025

Signature Name Title Date

Signed by:
Harihar Subramanian
80AF77615B5742F...
arihar Subramanian Regional CFO 4/8/2025

Signature Name Title Date

COUNTY OF ORANGE, A political subdivision of the State of California

COUNTY AUTHORIZED SIGNATURE:

Deputy Purchasing Agent

Signature Name Title Date

APPROVED AS TO FORM:

County Counsel

DocuSigned by:

By: Christine Nguyen
26F9D76C929A49E...

Deputy

Name: Christine Nguyen

Date: 4/9/2025

* If the contracting party is a corporation, (2) two signatures are required: one (1) signature by the Chairman of the Board, the President or any Vice President; and one (1) signature by the Secretary, any Assistant Secretary, the Chief Financial Officer or any Assistant Treasurer. The signature of one person alone is sufficient to bind a corporation, as long as he or she holds corporate offices in each of the two categories described above. For County purposes, proof of such dual office holding will be satisfied by having the individual sign the instrument twice, each time indicating his or her office that qualifies under the above described provision. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signator to bind the corporation.

ATTACHMENT A
SCOPE OF WORK

1. Purpose

This document is the Statement of Work (SOW) for a two-year service and maintenance extension of the existing Common-Use System Equipment (CUSE) and related server infrastructure at John Wayne Airport (JWA) starting June 1st, 2025.

SITA's responsibility for the existing CUSE system is comprised of the following primary systems and support staff, as described below.

1) Common Use Self Service (CUSS) kiosks.
2) Common Use Passenger Processing System (CUPPS).
3) A Site Administrator covering airport operating hours, seven days per week, and supporting planned maintenance, IT, and construction activity.
4) Multi-User Flight Information Display System (MUFIDS).
5) Resource Management System (RMS) and associated RMS/MUFIDS database.

The following equipment, software, and hardware changes and updates are necessary to extend the usable life of the systems and must be completed within eight months from execution of this contract. Additional details are included in the Scope of Support and Maintenance section of this contract. The following work must be coordinated with JWA IT prior to start:

1) Ensure all Windows and Server operating systems have the latest supported operating systems and service packs from Microsoft.

The following strategies are optional and can be exercised to extend the usable life of the systems after coordinating and receiving approval from JWA IT:

1) Optionally, replace various peripheral components that are considered to have decreased performance or should be replaced for health and safety reasons, such as ADA compliance, ergonomic requests approved by JWA.

Unless specifically stated, existing components and procedures will continue to be utilized under this Support and Maintenance contract.

1.1. Location of Work

All work activity within this SOW are offered on the basis that a contractor's license is not required for performing on site work at JWA. For any work that is subsequently found to require a contractor's license, SITA IPS reserves the right to subcontract a vendor who has the relevant license and submit a Task Order request for the additional charges incurred, or request JWA complete the required work.

Where equipment has to be accessed for upgrades or replacement, this work is assumed to be undertaken collaboratively by SITA and JWA staff, as needed.

SITA IPS supplied software upgrades, support, and maintenance and OS related tasks can be performed remotely via site-to-site VPN access, and must comply with the County of Orange Information Technology Security Provisions. JWA will facilitate appropriate secure remote access to SITA IPS and SITA for such works. SITA will provide VPN connectivity requirements to JWA.

1.2. Definitions

For the purposes of this document, the following terms may be used interchangeably:

- "SITA," "SITA IPS," "Vendor," or "Contractor" shall refer to SITA IPS and its agents, subcontractors, and anyone else they employ for the ongoing maintenance and support of the CUPPS environment and all of its components in accordance with this contract.
- "JWA," "Airport," and "County" shall refer to John Wayne Airport and its employees, agents, and any subcontractors utilized to ensure the ongoing continuity of operations of the airport and to satisfy its obligations in this contract.
- "CUPPS" shall refer to all collective components of the system including, but not limited to, CUPPS, CUSS, RMS, and FIDS.

1.3. System Owner, Stakeholders, and Users

The following are defined to clarify entities involved with CUPPS:

- System Owner: JWA, County of Orange
- System Contractor: SITA IPS (Refer to Section §2.3 for SITA Roles)
- System Stakeholders: JWA IT, OCIT, TSA, current and future JWA passenger air carriers.
- System Users: JWA passenger air carrier employees, air carrier customers, and others who directly interact with the services that the system provides.

1.4. Additional Work

1. 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.
2. 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.
3. 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.
4. Contractor shall continue to provide services to all areas not affected by work provided by alternate sources.
5. 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.

1.5. Reimbursable/Travel

Travel reimbursements shall not exceed the per diem rates established by the U.S. General Services Administration (GSA) for the primary destination. Maximum per diem reimbursement rates for lodging, meals, and incidental expenses are established by city/county and may vary by season. It is the Contractor's responsibility to review the current rates at www.gsa.gov and obtain the Project Manager's approval prior to travel.

2. Support and Maintenance Details

2.1. Scope of Support and Maintenance

SITA will provide support and maintenance for the CUPPS system components and management of the maintenance strategy for the equipment detailed in Section 5, Bill of Materials.

All physical networking infrastructure is supplied by JWA and supported by JWA. SITA's support and maintenance delimits at the network access point connection, which is provided by JWA.

SITA is responsible for the configuration of the CUPPS physical and virtual network interface cards.

All power is supplied by JWA and supported by JWA. SITA's support for any powered device includes any low-voltage power supplies, the AC power cord and plug, up to the point where it plugs into either a UPS, PDU, or main socket.

2.1.1. Support Provision Overview

SITA IPS has a team dedicated to support all of the systems and services that it has supplied. This team will be responsible for providing support to all JWA based users and users of the system. The objective of this team is to conduct preventative maintenance actions, promptly respond and repair the system in the event of system disruptions as described in section 3 of The Service Level Agreement (SLA), advise JWA of future software and hardware updates well in advance for planning purposes, and ensure the system is in compliance with regulatory and industry standards.

As part of this support agreement, SITA IPS's support team will ensure that service is restored within the defined SLA times from the logging of a call with the SITA IPS Service Desk. During any period of significant loss of service, the SITA IPS support team shall provide regular status updates to JWA and users to inform on troubleshooting actions, and the estimated time of repair to full operation.

SITA IPS shall provide monthly reports to JWA detailing system discrepancies, root cause of discrepancies for trend analysis, and how the discrepancies were resolved. SITA IPS shall also report discrepancies, such as software faults, and track the handling by the SITA IPS software engineering team.

Key features of the SITA IPS support package for users must include:

- 24x7 daily Service Desk operations
- Call logging and fault clearance tracking and reporting
- Prompt and defined response to all queries raised
- Fault priority and escalation procedures
- 24x7 infrastructure performance monitoring
- Response and Resolution times within defined SLA times
- On Site Administrator / Account Manager
- Additional Site Administrator

2.2. Service Delivery

SITA shall continue the established collaborative service delivery methodology, incorporating SITA's resources working alongside JWA's IT Support Team. This collaborative approach is directed and managed by SITA's Site Administrator / Account Manager, who is responsible for achieving SLA compliance with the resources available.

SITA shall provide appropriate training, diagnostic tools, and advice to the JWA IT Support Team to deliver the required level of incident resolution and preventative maintenance.

SITA will provide updates on the status and success of service delivery through the regular Service Delivery Review meetings.

2.3. Role Accountabilities

The following roles collectively make up SITA's Service Delivery capability for JWA.

2.3.1. Vice President of Operations, North America

Overall end-to-end accountability for SITA's Service Delivery approach.

2.3.2. Service Account Manager, North American

The Service Account Manager shall assist with any concerns for the duration of the contract. The Service Account Manager shall serve as a direct escalation point regarding questions or concerns, monitor performance of the supporting teams and expedite delivery of the various service requests, as needed. They will also provide support for the overall product performance and act as a liaison with other departments within SITA, as necessary.

2.3.3. Site Administrator Job Description and Duties

SITA will provide two (2) full-time site administration positions for JWA. These individuals will support CUPPS and CUSS, Airlines, and others ("Stakeholders") as defined in the job duties, functions, and responsibilities listed below. This will ensure continuity of operations and ensure delivery of the technical changes to the JWA CUPPS system as described in the SITA and JWA contract and this SOW. All activities will be in complete coordination with the JWA IT Manager and local JWA Support Team. The SITA site administrators will manage the site during JWA operational hours. The SITA site administrator's on-site operational hours will be scheduled in collaboration with JWA. The schedule will consist of one (1) individual for eight (8) hours per day occurring seven (7) days a week. The SITA site administrators will alternate offsite support to ensure coverage is provided to assist the 24/7 SITA Service Desk with Critical or Important issues as defined in Section 3.2.1, Priority Classifications, scheduled and recurring maintenance, and any upgrades that impact the CUPPS. SITA and JWA agree that schedule coordination should be handled locally and agreed upon between SITA VP of Operations and JWA IT Manager.

The agreed service level agreements for response and restore times are defined in Section 3.4, Service Level Agreement and Invoice Deductions.

Monthly, Quarterly, and Bi-Annual meetings as defined in Section 3.18, Service Meetings, will provide the forum to review schedules, SLA and technical issues as well as future work (e.g. power outages) in the next month or quarter. These meetings will ensure that SITA and JWA Manager remain engaged in schedule planning, SLA reporting, and any other topics related to SITA's scope of work. Meeting schedules can be adjusted as needed as mutually agreed upon between County and SITA.

Using the diagram in Section 3.2.3, Incident Process, both the site administrators and the JWA Support Team will be contacted by the SITA 24/7 Service Desk when calls and tickets are registered from JWA airlines or other authorized callers from JWA. JWA Support Team will be contacted for hardware issues and the Site Administrator will be contacted for software and server related issues. This also applies to work efforts needed for 3rd level support needed from the SITA Technical Engineers and Development support. This escalation and coordination process is for all systems supported by SITA.

SITA will ensure that the required Site Administrator(s) are hired and they have completed the JWA ID Badge process 30 days before the start of the contract. Reference **Section 65, Airport Security** of this contract for Airport ID/Access Control requirements, fees, and timeline. This is to ensure training has been completed. Site Administrators must have 1 year of IT industry experience. SITA will also ensure that if a Site Administrator is on leave that SITA will provide additional onsite coverage for the days of leave. This will also apply to a Site Administrator Account Manager who is terminated. These situations will be discussed at the monthly meetings with JWA IT Manager. County reserves the right to approve or reject on-site SITA personnel prior to job offer.

The following describe the functions of the Site Administrator. There may also be changes to this functional list of requirements based on operational and/or technical issues that arise at JWA. These changes to or additional work functions shall be mutually agreed upon between SITA, VP of Operations and JWA IT Manager.

1) Located at JWA with office space provided by JWA.
2) SITA's on-site interface to JWA, reporting duties to SITA IPS USA HQ
3) Provide direction to JWA's local Support Team in delivering service to the end user.
4) Site Administrator will recommend spare management. Spares will be purchased by SITA under Task Order budget with JWA or JWA direct purchase.
5) Site Administrator will be the airline and JWA's main point of contact and first escalation point for the functional topics as defined in this list of job functions.
6) Ensuring shortest possible restore times escalations to SITA specialized resolver groups, when necessary.
7) Communicating with the airlines and JWA to understand business and technical requirements.
8) Maintain accurate records pertaining to the inventory and all relevant account documentation.
9) Resolve complaints and prevent recurrence of repetitive issues.
10) Extensive product knowledge of airline systems and common use systems.
11) Regular meetings with airline station managers to discuss CUPPS, CUSS, and MUFIDS/RMS projects.
12) Regularly monitor status, health and performance of the CUSE servers, ensure applicable patching is performed.
13) Check and validate any alerts received from SITA monitoring system and ensure findings are reported back to SITA HQ for support, as required.
14) Network testing to the Airport demarcation point, when required, for fault finding for CUPPS workstations.
15) Determine source of network issues (local or host).
16) Triage network configuration issues with both airline IT and JWA IT.
17) Perform Disaster Recovery monitoring and execution, as required.
18) Pro-active monitoring of all systems to discover any issues that might have negative impact on service and infrastructure operations.
19) Following CUSE workstation setup plans, maintain commonality throughout the CUSE environment.
20) Assist with implementation of new airlines, agents and airline applications on the CUSE system and updates for existing airlines, when needed.
21) Provide assistance in setting up workstations or replacing on the CUSE platform.
22) Update, add and remove common use certified airlines and required peripherals on the CUSE platform.
23) Assist various support levels with fault-finding activities for airline systems when reported.
24) Act as hands and feet for remote support and service engineers, as necessary.
25) Provide supporting role in JWA change management process, as necessary.
26) Conduct required diagnostics and report and escalate technical problems, which cannot be readily resolved and track through to resolution.
27) Provide support for power outages, either scheduled or non-scheduled, as required.
28) Provide support for CUSE platform maintenance, either scheduled or non-scheduled, as required.
29) Regular and ongoing onsite equipment repair for peripheral equipment devices to

maintain adequate and recommended "working" spare quantity listed in 5.1.1.

30) Process MUFIDS and RMS changes and implement images.
31) Provide support and lead cybersecurity program and compliance efforts for all components within the CUPPS at the direction of County's IT Security Manager.
32) 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 CUPPS/CUSS systems.

2.3.4. Changes to Existing Equipment

The following equipment, software, and hardware changes and updates are necessary to extend the usable life of the systems and must be completed within eight months from execution of this contract. The following work must be coordinated with JWA IT prior to start:

1. Ensure all Windows and Server operating systems have the latest supported operating systems and service packs from Microsoft.

2.3.5. SITA Service Desk

SITA's Service Desk operates 24 hours a day, 7 days a week and 365 days per year. The Service Desk shall accept emails or phone calls for failure reports from JWA and other stakeholders, and for each call opens a trouble ticket. The trouble tickets are stored in a customer-specific database with customer-specific history for further investigation by the technical team.

Once the trouble ticket is logged into the reporting system, technical support will take the next step of investigation to determine the root cause of the reported problem. Failure reports and trouble tickets can be reported to SITA using the following email address and/or phone number.

How to Contact Us: SITA/Support Inquiries

- Email Support: SSD.Application@sita.aero
- Phone Support: +1 (866) 588-0497 / Customer ID Number 222

JWA will be informed about the result of the analysis and will receive a hot fix if the reported problem was a genuine software problem. JWA to have the capability to access reporting.

JWA will receive daily emails documenting any tickets that remain open from the previous day, and a weekly email documenting any tickets that remain open from the previous week.

2.3.6. Local JWA Support Team

Local JWA IT teams will continue to provide Level 1 on-site support.

1) SITA Site Admin will address any resource concerns with CUPPS Sr. Technologist or IT Manager.
2) Based on-site at JWA between the operational hours of 05:00-22:30 x 7 days per week
3) Expected to address CUPPS/CUSS 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.
4) Are first responders when on-site response required as directed by the SITA Service Desk personnel
5) Will provide timely responses to the SITA IPS Service Desk through email to document when an incident ticket is acknowledged and resolved.

6) Responsible for escalating incidents to the SITA Site Admin through the Service Desk by routing incident tickets to L2 Site Admin support.
7) Responsible for providing feedback to users on fault resolution
8) Responsible for initial resolution of user issues such as log in, program access, peripheral access, replacement of defective peripheral hardware
9) Responsible for delivering Planned Hardware Maintenance schedule recommended by the SITA Site Admin, who is responsible for escalation and coordinating resources from other third-party suppliers (i.e., OCIT/SAIC).

3. Service Level Agreement

3.1. Services

SITA IPS will perform the scope of services defined below in order to meet and exceed the service levels that are applicable to all common-use systems currently in operation at JWA, and prevent/ eliminate faults as defined in the Service Level Schedule.

The Service Level Agreement (SLA) services provide:

1) Levels of service provided by SITA IPS to JWA for support of the accepted production version of the deliverables in accordance with the terms and conditions of the Agreement.
2) The fault maintenance process for software components produced by SITA IPS. Enclosed third party software components will be covered by appropriate servicing contracts, under the management of SITA. Supplied software is listed in the Agreement.

The JWA CUSE infrastructure is continuously monitored from SITA's 24x7 remote team. Any housekeeping or potential fault rectification will be performed outside of operational hours as much as possible in coordination with JWA and County IT. Variances from this requirement shall be mutually agreed upon between Vendor and County.

SITA requires the JWA Support Team to be available on site during operational hours and support the required SLA conditions. In the event that an SLA is unresolved due to the unavailability of the JWA Support Team (or due to conflicting priorities outside of the control of the SITA Site Administrator) then JWA's unavailability shall not incur penalties and will be tabled for discussion at the next scheduled Service Review meeting.

3.2. Description of Service Levels

A priority classification will be assigned to each incident reported at time of initial contact to the SITA Service Desk. These priority levels are based on severity of the problem, business, operational or reputational impact to the JWA and the traveling public. Priority levels will need to be agreed by both SITA IPS Service Desk and the reporting party in order to determine appropriate response/resolution times. The assigned service level is confirmed to the requestor via email. If the priority of the problem requires adjustment, the requestor or other authorized JWA authority will contact the SITA Service Desk, identify the report or incident in question and request change of priority classification. The fault(s) description(s) and other pertinent information will be kept in SITA IPS's ticketing system and relayed to JWA during the regular reporting cycle.

3.2.1. Priority Classifications

Problems shall be managed according to the severity of the problem. The following table provides a description for the different priority level categories:

Priority	Description	Examples
Priority 1: Critical	The entire system is completely unavailable, or performance problems are preventing use of the system.	No workstations or kiosks are available to process passengers. Major server / service outage.
Priority 2: Important	The system or a sub-system is partially disrupted, or is experiencing performance issues, but overall functionality is still available.	All kiosks down in a particular terminal or for an airline. Partial disruption to one or more airlines operating ability. Performance issues resulting in very slow transaction processing time, **for example**, server response time that are greater than 250ms per individual click.
Priority 3: Low Priority	The system or a sub-system has minor issue with minimal or no impact to the daily operations.	Single or few desks/kiosks/MUFIDS are impacted or intermittently unavailable. Peripheral and/or hardware failures.

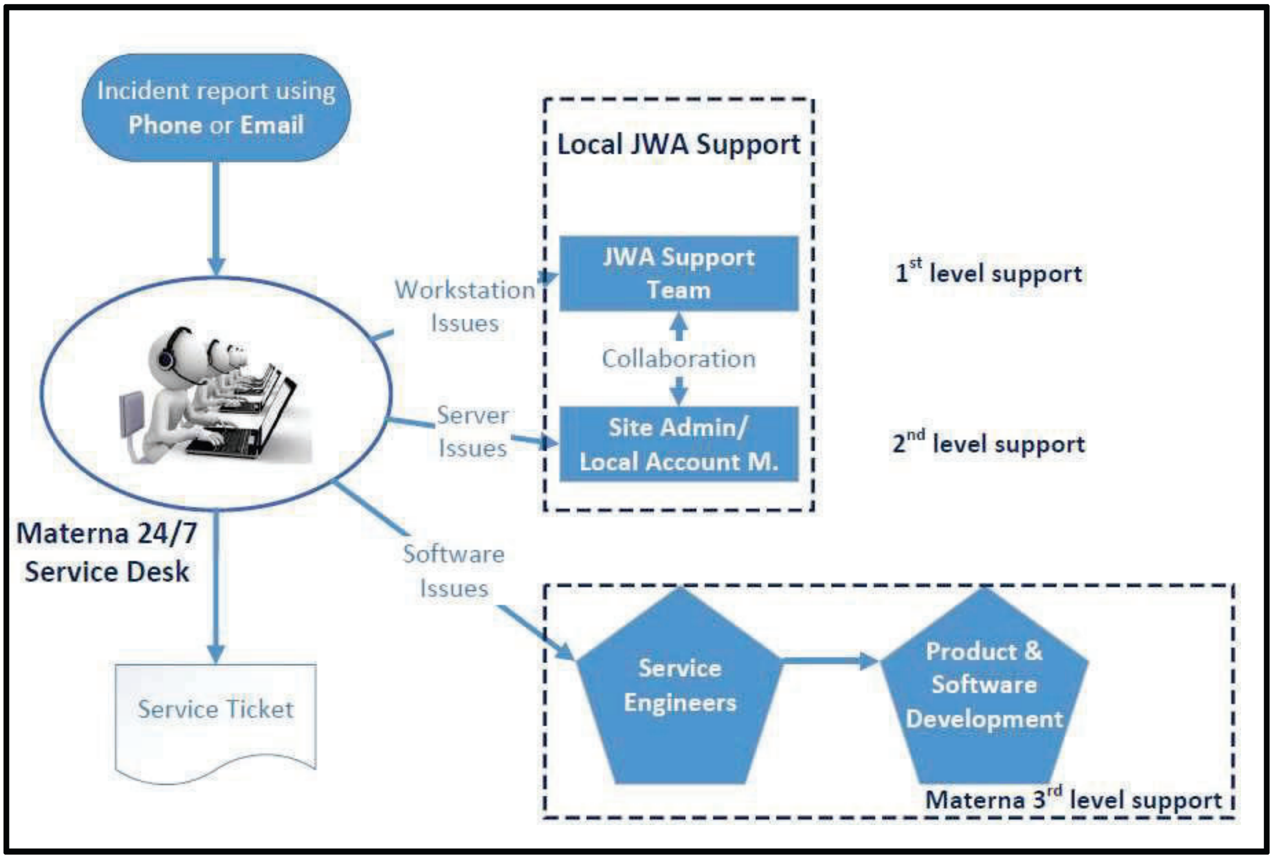
3.2.2. Incident Management

The purpose of Incident Management is to return the system in question back to service, enabling the customer to continue to use it, restore to normal operation as quickly as possible, and minimize the adverse impact on business operations thus ensuring the best possible levels of service quality and availability are maintained.

To carry out incident management, SITA has a team available on a 24x7 basis, to own and manage incidents through to resolution.

3.2.3. Incident Process

SITA will provide 24/7 support for JWA and its users via the SITA Service Desk. The Service Desk will make best efforts to collect all necessary information based on caller information. The Incident Report Form (Appendix A) outlines all information that is expected for efficient resolution, at the time of placing the incident report. Upon first contact, the service desk will identify the nature of the issue, log all of the provided details into SITA's internal service management tool and escalate to the appropriate party for resolution. A simplified diagram of the various support teams and incident escalation process can be found below:



SITA Service Desk: SITA IPS Service Desk provides a single interface to JWA. SITA IPS Service Desk requires that all information regarding the incident be accurately provided at the time of the call or in the email sent to the Service Desk. SITA IPS Service Desk then creates a trouble ticket and dispatches the trouble ticket to the Local JWA Support team for hardware issues. Trouble tickets related to system recovery including but not limited to restarting kiosks, servers or other communication equipment will be escalated to the L2 Site Admin at JWA. Problems that cannot be resolved at this level will be escalated based on the nature of the incident.

JWA Local Team: All hardware and workstation issues (e.g. issues with peripherals, consumables, issues likely related to network and connectivity, etc.) will be escalated to the JWA Local IT Team for investigation and resolution. The JWA Local Support Team will do their best to provide final resolution to the issue. The Local Support Team will escalate to Site Administrator or JWA Networking Team as might be necessary.

Site Administrator: If the JWA Local Team is unable to provide resolution, they will seek further assistance from and provide details of their investigation to the Site Administrator based on the results of their investigation. The Site Administrator will continue to investigate and provide resolution or further escalate to specialists as might be necessary.

SITA 3rd Level Support Teams: All issues related to software and product problems (e.g. software bugs, performance problems, database, configuration, etc.) will be escalated to the 3rd level support teams, based in both the U.S. and Germany. These teams provide remote support and assistance to various sites and are assigned their tasks based on the priority levels of various incoming requests. The 3rd level support consists of the following main functions:

SITA Service Engineers Team: SITA IPS Service Engineering Support is provided by SITA IPS's highly qualified service engineers. They have all the tools and knowledge base to analyze problems in detail including but not limited to evaluating traces, log files, and assist with PCI compliance items and audits. Service Engineering Support is provided remotely. Problems that cannot be resolved at this level will be escalated to Software Development Support.

SITA Product & Software Development Teams: the product specific development teams provide SITA IPS Product & Software Development. They analyze and correct software bugs and are responsible for the development of the platforms installed at JWA.

3.2.4.Support Response Teams Availability

For the Support, the following are the Service and Response Times:

Service	Availability
Service Desk*	**24 hours / 7 days**
Technical Support (Service Engineers Team)	15 hours / 7 days, 2030 – 1130 PST**
Development Support	10 hours / 5 days, 2230 – 0830 PST
* To carry out incident management, SITA has an on-call team on a 24x7 basis, to own and manage incidents through to resolution ** Technical resources can be made available outside of the above-described hours for specific service requests	

3.3. Escalation Process

SITA IPS generates a standard internal escalation process automatically.

Should the normal means of raising an issue be unsatisfactory, or the response received by the user not reasonably deemed to be adequate, the escalation path will be followed as shown below:

In addition to the defined service levels, the escalation process can be invoked automatically by certain rules, which are created in the service management tool for each individual site, such as a critical number or percentage of workstations, a particularly critical single item, or even by a certain time such as a busy day, time, or season. These rules are created in collaboration with the JWA or their nominated representatives during the project phase, and then reviewed regularly during normal operation as required with the Site Administrator.

Order of Escalation	John Wayne Airport	SITA IPS
1 Before expiry of Target Restore Time in case of P1 & P2 incidents	**Von Hester** Senior Technologist vhester@ocair.com +1 (949) 252-6064	**Site Admin / Account Managers**
2	**William Bogdan** IT Manager, Innovation & Technology wbogdan@ocair.com +1 (949) 375-2514	**Balázs Csongrádi** Head of Technical Solutions Balazs.Csongradi@sita.aero +1 (980) 666-9019
3		**Daniel Dunn** Senior Manager Infrastructure Management Daniel.Dunn@sita.aero +1 (202) 351-9647

If an outage exceeds the service levels, all interested parties will be notified. Furthermore, during an incident, should an SLA be breached, or close to being breached, the escalation process will be invoked.

3.4. Service Level Agreement and Invoice Deductions

In the unlikely event the incident resolution process is taking longer than the prescribed service levels and committed resolution times outlined, various financial deductions can be applied.

The table below shows the breakdown of possible deductions to the monthly invoice. JWA will present the SLA to be deducted from an invoice should SITA not meet the defined service levels within 10 business days of the occurrence. These deductions do not apply to issues outside of SITA's control or scope of responsibilities.

Overall System Availability Service Levels	
Unavailability of 2 or more major system functions to one or more airlines or site-wide for more than 15 minutes.	Offset: 1.5% of the amount billed this month for each (15) minute period or fraction thereof a system is unavailable.
Unavailability of any major application (CUTE or CUSS or CUPPS or MUFIDS) to one or more airlines or site-wide for more than 2 hours.	Offset: 10% of the amount billed this month for each (2) hour period (or fraction thereof) an application is unavailable.
Unavailability of any primary server for more than twenty four (24) hours	Offset: $2,000
Unavailability of any backup server for more than forty-eight hours (48).	Offset: $1,000
Gateway Availability	
Unavailability of any gateway system or external data connection for more than 24 hours	Offset: $1,000 per 24-hour period or fraction thereof
Workstation Availability (including attached required peripherals)	
Any individual workstation or kiosk not available for use for more than 24 hours.	Offset: $500 per 24-hour period or fraction thereof.
Any individual workstation or kiosk has 4 or more trouble calls in any 30-day period (+ 5 previous month days).	Offset: $300 per incident.
Gates with 2 workstations: Both workstations are simultaneously not available for more than 30 minutes.	Offset: $500 per one (1) hour period or fraction thereof.
Gates with 4 workstations: 3 or more workstations simultaneously unavailable for more than 30 minutes.	Offset: $500 per one (1) hour period or fraction thereof.
Display Availability	
Any individual CUTE workstation / CUSS kiosks / MUFIDS display not available for 72 hours.	Offset: $500 per 72-hour period or fraction thereof.
Response Time Exceeded	
Critical trouble call response time exceeds the defined time (below) (Priority 1)	Offset: $1,000 per incident
Important and Low Priority trouble call response time exceeds the defined time (below) (Priority 2 and 3)	Offset: $500 per incident
Critical Trouble Call Response Times (Priority 1)	

The on-site response time for a Critical Trouble Call during JWA hours of operation is two (2) hour or less between the time the problem is reported to SITA Service Desk and the time a Site Administrator is at site of trouble ticket location.	
The on-site response time for a Critical Trouble Call during JWA hours of non-operation is four (4) hours or less between the time the problem is reported to SITA Service Desk and the time a Site Administrator is on site.	
During JWA hours of operation, the remote services and diagnostics should commence within fifteen (15) minutes following notification to SITA Service Desk of a malfunction by JWA or by way of remote monitoring.	
During JWA hours of non-operation, the remote services and diagnostics should commence within one (1) hour following notification to SITA Service Desk of a malfunction by JWA or by way of remote monitoring.	
Critical trouble calls are to be resolved within twenty-four (24) hours following notification to SITA Service Desk of a malfunction by JWA or by way of remote monitoring discovery.	
Important and Low Priority Trouble Call Response Times (Priority 2 and 3)	
The on-site response time for Important (Priority 2) Trouble Call is four (4) hours or less between the time the problem is reported to SITA Service Desk and the time the SITA Site Admin / Account Manager is on-site.	
The on-site response time for Low Priority (Priority 3) Non-Critical Trouble Call is twenty-four (24) hours or less between the time the problem is reported to SITA Service Desk and the time the SITA Site Admin / Account Manager is on site.	
During JWA hours of operation, the remote services and diagnostics should commence within two (2) hours following notification to SITA Service Desk of a malfunction by JWA or by way of remote monitoring for Priority 2 calls and four (4) days for Priority 3 calls.	
During JWA hours of non-operation, the remote services and diagnostics should commence within two (2) hours of the start of the next day's hours of service operation following notification to SITA Service Desk of a malfunction by JWA or by way of remote access.	
Non-critical trouble calls are to be resolved within ninety-six (96) hours following notification to SITA Service Desk of a malfunction by JWA or by way of remote access discovery.	
JWA PCI audit reporting and response	
Provide the requested PCI documentation within two (2) business days. Offset: $500 per 24-hour period or fraction thereof	
On-site Coverage (Onsite technician must have at least 1 year applicable IT experience and able to perform all duties listed in 2.3.3)	
Absent onsite coverage hours greater than two (2) hours or more per week (of the 56 total) will result in a $125 per hour deduction. Schedule accommodations will be allowed for emergency situations with concurrence between JWA management and SITA VP of Operations (or their designee's)	
Remote work to substitute daily onsite hours is not an acceptable provision, unless there is a need for a rare event or under **extraordinary circumstances**, defined by the following as: by reason of acts of God, restrictive governmental laws or regulations or other cause without fault and beyond the control of the party obligated (financial inability excepted). These situations will require concurrence between JWA IT Manager and SITA VP Operations	
Miscellaneous Items	
Reports are not provided later than five (5) business days as required in the SOW or due to loss of data.	$500 per occurrence.

Service Desk does not answer phone calls, respond to emails within four (4) hours, or does not generate a service ticket within ten (10) minutes after completion of the initial phone call.	$1,000 per occurrence
Misclassification of priority levels on 4 or more service tickets in a 30 day period. Penalty shall not apply to tickets that increase in priority due to an evolving issue or due to lack of information from the caller.	$500 per occurrence

3.5. SLA Coverage

The SLA applies to the following systems and sub-systems as described in Section 4, *System Design Description.*

3.6. Support Precondition Requirements

JWA has legally purchased the licensed CUPPS and CUSS software or acquired an appropriate right to use the product. At any time, the software to be maintained under this contract shall be in original condition or modified by SITA only.

SITA IPS may reject maintenance and/or support, if, the licensed software has been modified by JWA or a third party without prior consent of SITA IPS.

3.7. Change Management – Planned Changes (Change & Configuration Management)

All changes will be correctly documented according to pre-defined process and must be fully approved by both parties.

A JWA IT Change Request Form (Attached) *(County of Orange Change Request Clause does not apply)* is also completed by the SITA IPS Site Administrator and submitted for approval to JWA. Normal Change Requests require a minimum 3 days in advance. If it is less than 3 days, then an Emergency Change Request is required and indicated on the JWA IT Change Request Form

SITA IPS and/or JWA will then communicate the required Change to all users in most cases at least 3 days prior to the agreed change date.

3.8. Unplanned Changes (Incident and Change Management)

Any change to the system, which is not planned as per the Change Management process is defined as an emergency change and is usually in response to an Incident.

All emergency changes must still be approved (by JWA IT, by a technical proposer and a SITA IPS representative) and completed in the service management tool after the event, with a link to the original incident.

All planned, unplanned, completed (and any failed) changes will be documented in the monthly service review document, presented by the Site Administrator – and, if required, can be supported by conference call by the relevant team. Information can also be requested "ad-hoc" through the Incident Management Team or via the Site Administrator.

3.9. Preventive Maintenance

SITA will fully train the JWA Support Team personnel in preventative maintenance for equipment delivered to JWA. SITA's Preventative Maintenance Program (PMP) is designed to keep the equipment running at maximum efficiency, thus reducing the number of faults encountered ensuring that day-to-day airline and airport operations are not disrupted. The results of PMP reduce incidents of equipment failure. Additionally, PMP regular activities result in cost savings for JWA.

The PMP is defined in Sections 3.9.1 to 3.9.3:

1) JWA provides the schedules based on the recommended PMP provided by SITA.
2) JWA's Support Team undertakes the PMP activities following the weekly, monthly and quarterly recommendations.
3) The JWA Support Team will ensure that SITA Site Administrator is aware of operational issues discovered during their PMP activities that may need to be addressed by SITA.

3.9.1. Self Service Check-in Kiosk Preventive Maintenance Activities

Monthly Checks

1. Clean screen
2. Check printer print quality
3. Clean Passport Reader, Barcode Reader, and Credit Card Reader
4. Monitor general condition & clean when necessary clean dust from vent holes
5. Test for normal operation

Quarterly Checks

1. Blow out dust from inside the kiosk and clear all dust from ventilation fans including pedestal fans
2. Calibrate touchscreen

3.9.2. Common Use Workstation Preventative Maintenance Activities

Monthly checks

1. Clean all dust from IGEL Thin Clients
2. Printers should be thoroughly cleaned inside and out, check the print quality and clean the print heads
3. Inspect all cables for any visible damage and worn parts
4. Replace ribbons and print heads as necessary
5. Boarding Gate Readers (BGRs) should be thoroughly cleaned
6. Blow dust away from beneath the keys on keyboards, Clean Magstripe Reader/Onboard Card Reader ("MSR/ OCR")
7. Clean Monitors
8. Test for normal operation

Quarterly checks

1. Inspect for heat damage
2. Clean all dust from IGEL Thin Clients
3. Calibrate eLO Monitors
4. Monitor general condition & clean when necessary clean dust from vent holes

3.9.3. MUFIDS Devices Preventative Maintenance Activities

Quarterly checks

- ✓ Monitor general condition of MUFIDS Screens and PC's
- ✓ Clean dust from vent holes and inspect for heat damage

3.10. Maintenance & Repairs of Equipment

The Site Administrator will undertake equipment repairs on an as needed basis. This means JWA will not have to buy warranty extensions if deemed unnecessary, only maintain existing / recommended spare stock levels for existing assets.

3.11. Out of Warranty Asset Maintenance (Task Order Process & Budget)

The responsible party for the replacement of Assets considered Beyond Repair and not covered by a Warranty will be as follows:

If any Asset fails after June 1st, 2023, then JWA bears responsibility for replacement, which will be executed via the Task Order Process or JWA direct purchase.

In either event, after the replacement of the failed device, SITA IPS maintains ongoing responsibility for managing the repair process (either locally or via warranty). SITA IPS shall also maintain an Asset register that clearly identifies each Asset and its corresponding Warranty status to notify JWA of the gradual warranty expiration period and recommend replacement per the County contract provision (EOL software/hardware).

In the event that the contractual cumulative task order value is exceeded prior to the end of the contract, then JWA bears responsibility for any additional costs.

Details of the total Task Order Budget are contained in the Pricing Attachment.

For clarification, the following items are assumed to be in the task order equipment list:

1. ELO Touch Screen – Ticketing & Gates / Spares
2. Handheld Scanners / Spares – Desko
3. Boarding Gate Readers / Spares – Desko
4. Lexmark 312 Document Printers / Spares – Lexmark
5. ET6500 Printers / Spares 2016 – Unimark
6. ET7000 Printers / Spares 2022 -Unimark
7. USB Serial Device
8. Integrated keyboards
9. 24" MUFIDS Display
10. 40" MUFIDS Display
11. 46" MUFIDS Display
12. 50" MUFIDS Display
13. 55" MUFIDS Display
14. MUFIDS RASPBERRY PI's
15. iGel UD2 thin clients
16. Kiosk enclosure
17. ELO Touch Screen – Kiosks / Spares
18. HP ProDesk 600 / Spares
19. Ingenico 4000 Payment Device kit (Card Reader, Keypad, Touchless Device) / Spares
20. DESKO PentaCube Document Scanner / Spares
21. KPM180H Custom Printer – Kiosk / Spares
22. Any effort required that is not a defined responsibility of SITA IPS's within this SOW

3.12. Equipment Spares Stock

It is recommended to maintain spare equipment in stock. Spare equipment stock maintenance recommendation levels will be determined between SITA and JWA on an ad-hoc basis.

3.13. Faulty Equipment Strategy

The SITA Site Administrator's will maintain faulty equipment. Faulty equipment will be removed from operational use and bench repaired using components held in spares stock or purchased as necessary. The SITA Site Administrator will advise JWA when additional spares stock or components need to be purchased to maintain the levels necessary to ensure the operational equipment can be maintained at the levels required by the SLA.

3.14. Configuration Management Database

SITA IPS's Service Delivery Team has the responsibility to maintain the Configuration Management Database (CMDB), which is used under normal change control. The configuration items held for the service provided at JWA include the airline applications (and version numbers) installed, the server platform software versions and licensing, and other important configuration items recorded as part of the change process.

The CMDB is available via SITA IPS's service management toolset in read only format to the Site Administrator for reference purposes. JWA may request information reporting from this database on an ad-hoc basis.

3.15. Consumables Management

The following items listed in table below are considered consumables and are paid for by JWA.

Consumable Item	Monitored & Ordered By	Installed By
Bag Tag Stock	JWA	JWA
Boarding Pass Stock	JWA	JWA
Laser Printer Paper	JWA	JWA
Laser Printer Toner Cartridges	JWA	JWA
Laser Printer Drum Cartridges	JWA	JWA
Kiosk Paper	JWA	JWA
Cleaning Materials	JWA	JWA
Specialist Service Tools	JWA	n/a
Unimark Print heads and Platen Rollers	JWA	JWA
UPS Batteries	JWA	JWA

3.16. Monitoring

A combination of the following 3rd party tools will be used to provide in-depth monitoring of the CUSE back- end infrastructure. These tools are:

1. **Icinga** – SITA's monitoring tool is already in use for monitoring the CUSS kiosks for JWA CUPPs technicians and staff via email alerts. This will be further extended to the CUPPS servers and workstations.
2. **Tripwire** – This specialized 3rd party tool is already installed and configured to meet PCI DSS requirements for file integrity monitoring (FIM) for all CUPPS/CUSS devices including servers. SITA shall provide services and monitoring.
3. **Mosaic451/Sentinel** – Security log monitoring service provided and monitored by JWA. This is installed on all devices (Servers, CUSS endpoints and CUPPS). Mosaic451/Sentinel programs monitors Window Event Logs, Application Logs and System Logs.

The combination of the above software tools, pre-defined, and agreed monitoring criteria between SITA and JWA will ensure all required system metrics are covered, and will provide real time information of health status and PCI compliance.

Icinga alerts generated will trigger engineers to perform investigations and report to JWA as part of the usual monthly reporting, or in real time depending on the severity of any incident.

Alerts can be configured and distributed to JWA users as required. The following elements of the system will be monitored:

1. Server and Storage Hardware and Connectivity Faults;
2. Windows Services;
3. Windows Event Logs
4. Resource Utilization (CPU, RAM, Network, I/O); and

5. Network Connectivity (VLAN availability, airline circuit availability)
6. Virus Alerts
7. Application Logs
8. System Logs
9. File Integrity Monitoring (Tripwire)
10. Veeam backup Service Monitoring

Security log alerts will be monitored and stored by JWA for PCI auditing purposes.

3.17. Reporting

SITA IPS will provide monthly reports detailing incidents and service requests, containing the following items per fault:

1. Time of call to SITA IPS.
2. Call reference.
3. Location of fault (unique device identifier).
4. Details of fault reported.
5. Equipment type affected.
6. Airline
7. Action taken by Service Desk (e.g., passed to engineers).
8. Time of action taken by Service Desk.
9. Engineer's name (reference).
10. Descriptive details of fault found (dependent on Airline or JWA provided details)
11. Descriptive details of repair (dependent on Airline or JWA provided details)
12. Time resolved.(dependent on JWA or SITA technician ticket closure accuracy)
13. Engineer's comment
14. For CUSS Kiosks: time from initial Icinga alert until the item is cleared within the system.

The SITA IPS Site Administrator also compiles a Monthly CUPPS Usage Report to accompany the Monthly Service Report. This report is sent to the JWA IT Manager, SITA IPS Head of Service and Support and Head of SITA IPS Service Desk Operations for review and approval. Once agreed and finalized, the Head of Service and Delivery submit these reports for payment.

SITA IPS will continue to compile and present the service level compliance report on a monthly basis to key JWA users. The report will be made available prior to invoicing and the onsite account manager will be made available to discuss any concerns and address any preventative measures.

Reports for previous month are due by the 7th of the following month. (i.e. January monthly reports due by February 7th).

3.18. Service Meetings

SITA IPS will hold the following meetings with JWA as a mechanism for review of service performance.

3.18.1. Monthly Service Reviews

The following agenda items need to be covered in the Monthly Service Reviews.

1. Comprising SITA Site Administrator and JWA Sr. Technologist and IT Manager.
2. On-site meeting at JWA.
3. Review Service Performance during the previous month.
4. Review SLA Compliance Report.
5. Review Patching and vulnerability status (for PCI compliance).
6. Review PCI monthly checklist.
7. Review compliance with Planned Maintenance Program.

8. This meeting will also review upcoming Project delivery tasks in consideration of ongoing operational management of the CUPPS system and available spare capacity of the JWA Support Team.
9. Staffing coverage and/or upcoming planned absences for site Admin(s).

3.18.2. Quarterly Technical Board Meetings

The following is the proposed agenda for the Quarterly Technical Board Meetings.

1. Comprising of SITA's Site Administrator, SITA's functional managers (as appropriate) and designated JWA individual(s).
2. On-site meeting at JWA and/or conference call.
3. Review Application updates available from SITA IPS.
4. Discuss ideas concerning improving technical or functional capability of the system.
5. Review PCI/Vulnerability program, or on an ad hoc basis, as necessary.

3.18.3. Bi-Annual Executive Meetings

The following is the proposed agenda for the Bi-Annual Executive Meetings.

1. Comprising SITA President of Americas, SITA VP Operations, and JWA staff as appropriate.
2. On-site meeting at JWA and/or conference call (at JWA's discretion).
3. Review issues or concerns arising from both the Monthly Service Review and Technical Board meetings.
4. General review of performance against expectations.

3.19. PCI DSS Audit Support

SITA's responsibility under the contract is to provide support for the annual PCI DSS Audit against the requirements in PCI DSS latest active version. SITA's PCI areas of specific responsibility are outlined in the CUPPS PCI Matrix of Responsibilities (Appendix B), attached by reference due to confidential sensitive security information. The amount of PCI DSS Audit support hours required e.g. the provision of evidence; screenshots, logs, and interviews to the auditor for up to 25 days of effort annually is included in this scope of work. Labor exceeding 25 days annually will be billed to the County per preapproved task order.

SITA shall maintain the CUPPS platforms' in a manner capable of supporting PCI DSS compliance. PCI DSS compliance for the avoidance of doubt means:

1. System is installed in a compliant manner
2. System is maintained to be compliant
3. Deficiencies are remedied at no charge, if they fall within scope of the contract

Changes in the PCI DSS specification that result in CUPPS system changes (which may include procurement of additional hardware or software) will be recharged to JWA.

In the event the PCI DSS requirements are conflicting with IATA CUPPS / CUSS standards, these conflicts will be discussed with JWA so a mutual resolution can be reached.

Provide monthly PCI DSS checklist 12.11 to attest service provider (SITA) is performing their services for the JWA CUPPS system stated in the Statement of Work related to PCI Compliance.

3.20. Operating Systems

3.20.1. Windows 10 and Windows 11

Windows 10 is the current operating system. SITA will assess Windows 11 for compatibility and readiness of the airline applications and communicate with airlines and County on the feasibility of implementing the new OS before Windows 10 reaches end of life on October 14, 2025.

4. System Design Description

[redacted].

4.1. [redacted]

[redacted].

[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1. [redacted]

   [redacted]

2. [redacted].

[redacted]

3. [redacted]

4. [redacted]

4.2. [redacted]

[redacted]**:**

[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

4.3. [redacted]

[redacted]

[redacted] [redacted]
[redacted] [redacted]
[redacted] [redacted]
[redacted] [redacted]
[redacted] [redacted]
[redacted] [redacted]
[redacted] [redacted])

[redacted]

4.4. [redacted]

[redacted]

4.5. [redacted]

[redacted]

4.6. [redacted]

[redacted]

5. Bill of Materials

This section defines the Bill of Materials (BOM) that are installed at JWA at the SITA IPS, USA takes over this contract.

5.1. CUPPS Workstations

JWA has and SITA IPS CUSE Enterprise (virtualized) installation of 245 thin client workstations with the peripherals connected via USB-Serial converters. The location of these workstations are as detailed in the below table:

Equipment Type	Location	Quantity
Agent CUSE Positions	Jet Bridge Gates	20 x 4 = 80
	Commuter Gates	2 x 6 = 12
	Sky Caps	3 x 6 = 18
	Ticket Counters	3 x 38 = 114
	Federal Inspection Services (FIS)	1 x 4 = 4
	Customer Services	5 x 2 = 10
	Training / Preproduction	1 x 7 = 7
	Total	**245**

All workstations are fully common-use, available to all airlines with the same features respective to their locations.

5.1.1. Peripherals at JWA

The following provide the type and quantity for peripherals based on information received from SITA.

Hardware/Peripherals	Qty	Picture	Functional Spare Qty
iGel UD2 Linux thin client	240		3% (8 pcs)
Desko keyboard	245		3% (8 pcs)
Unimark ET6500 printer (EOL will be replaced by ET7000)	423		3% (14 pcs)
Unimark ET6500 printer with RFID module for Delta Air Lines	24		10% (2 pcs)
Desko/Honeywell 1900G Boarding Card Reader	245		3% (8 pcs)

Hardware/Peripherals	Qty	Picture	Functional Spare Qty
Desko 604 Boarding Gate Reader (BGR)	60		6% (4 pcs)
Unimark ET7000 printer	423		3% (14 pcs)
Lexmark MS312DN	47		3% (2pcs)

5.2. CUSS

Equipment Type	Location	Quantity
CUSS Kiosk Positions	Lobby	38 x 3 = 114
	Baggage Claim	1 x 2 = 2 (A & B only)
	Customer Services	A, B, C = 8
	Lab	1 x 1 = 1
	Spares	7 + 18 = 25
	Total	**125 (Not Including Spares)**

5.3. Kiosk Component Spares

The following table shows the kiosks spares that currently exists and is deemed sufficient for the life of the SOW.

Device	Percentage Spares	Qty Spares
HP ProDesk PC	3%	5
19" LCD Touchscreen	3%	3
Internal service keyboard	3%	9
Speakers and amplifier	3%	9
3M passport reader	3%	2
Custom KPM180 printer	19%	50

5.4. Multi-User Flight Information Display System

The MUFIDS will be designed in a way that facilitates a hands-off approach. It will function with as little manual intervention as possible. Specifically, flight information for airlines at JWA should be populated and updated automatically via JWA's OAG / Flight view data source. A hosted server will be provided by TSI. System configuration will be done through a web interface accessible by any authorized user on the appropriate network. Flight information will be displayed on monitors to be located throughout the Airport for a total of 350 displays.

The MUFIDS system will be networked to connect to the cloud infrastructure. These are secured within the application. No other dedicated connectivity is required, however; outbound TCP ports 80/443/8080/9915-9917/8034-8037 will need to be opened.

The MUFID System:

1. Shall allow basic configuration through a standard web browser.
2. Shall have access control, with adjustable permissions and logging.
3. Shall be able to export live data to be displayed on the Airport's display system
4. Shall have display interfaces that are remotely configurable, and only require power and network connectivity to function.
5. Unlimited user log in. Secure and tiered security access allowing 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 a Gate from its owner and for the Owner to either Accept or Reject that request with a Reason.
6. Shall be simple and intuitive so that appropriate airline employees can view or modify information with little training.
7. Shall be easily expandable, so that adding a new display does not require extensive configuration.
8. Shall have the ability to display data in multiple languages.

5.5. Resource Management System

The RMS system is a web-based solution hosted, served and run on cloud infrastructure. When using the system, users connect to the cloud and run the RMS application over a secure internet connection using https encryption on port 443 (https), no other port or connection is required. Each airport is given a specific airport domain(s) that they use to access the cloud system and these are secured by individual firewalls with strict port controls and access, increasing the security of the application.

RMS includes:

1. Real Time Data (From OAG) into the system to produce a gate plan (Gantt chart) based on airport-specific rules.
2. Creation of centralized data base
3. Ability for the system to send alerts 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 -Ability to change the rules per gate within the system
6. Automatic warning when rules are broken
7. Ability to add or remove gates and add remote hardstand areas to show in the system's Gantt chart.
8. Unlimited user log in. Secure and tiered security access allowing 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 a Gate from its owner and for the Owner to either accept or reject that request with a Reason.
9. Map based view showing gate assignments in real time over a 24-hour period.

Additional RMS features excluded from the base package that are available as add-ons:

1. Forecast tool and future stand planning.

2. Stand outage management and planning of outages shown within the system for scheduled closures or temporary maintenance.
3. Tow Management allows airport to define and readily setup tows against specific flights and allocations, using simple point and click on the Gantt chart.
4. Mobile FIDS
   AeroCloud FIDS solution is a new lightweight customer facing application providing detailed flight information via mobile devices. The mobile solution comes with the capability of tracking flights, filtering flights by destination, commercial/concession opportunity, parking opportunity and airport information in one application. This can be automatically branded in specific airport themes when a consumer is within a certain geofenced area of the surrounding location of the Airport.
   a. The App is supplementary to the current incumbent FIDS system and is not a replacement of it.
   b. Comprises of 3 main features/screens – our initial view is Flight Data and Status, Map with location and Notifications with user driven scope to add more if needed.
   c. All data will be derived from the central database within the IAM platform. Published via our own Aero Cloud Store Account(s).
5. Intelligent Airport Management
6. Future planning element (beyond 7 days included in base package)

5.5.1. Gate Management Module

When a user logs in and access the Gate Management function, they are presented with the live Gantt chart display for the current day, which can be easily changed to any other date of their choice. The live plan on any chosen day is updated automatically in real time as underlying data is updated, without the need of manual refresh on the display. This feature draws user attention to live updates by visually highlighting allocations and flights that have recently changed on the Gantt chart.

AeroCloud RMS also presents the Gate Assignments in a Map View format so user is able to see physical occupancy of gates for any time of day or date.

The RMS system supports multiple organization structures and access control upon them. In the case of JWA, each separate department can be treated as a separate organization if they manage separate gates or have separate department users managed under one overall organization. There is no limit to the number of organizations that can be created in the system and each are able to update the Gate Management system simultaneously without restrictions.

Within the Gate Management Module, there is the ability to setup and define the airlines and "owners" of specific gates via the organization administration function. Depending on how the airport wants to operate the Gate Management Module, there is an ability to allow external airline users direct access to the system with the ability to manage their "own" gates. This control is via organizations and provides a powerful feature to control who is able to manage and operate a specific set of Gates. It is not mandatory that the system is configured in this manner by the airport, but it demonstrates the flexibility of the system to allow different types of users from different organizations to have controlled access into the Gate Management Module.

All data, historical or day of operations, + 7 days into future, is stored online. Users can easily revisit a point in the past using the main Gantt chart by selecting a date they wish to look at. This provides the ability to look at any historical data within the system without the need to load archive files etc.

5.5.2. Central Flight Management Module (IAM)

The Central Flight Management Module allows real-time view of operational flights and its data elements.

Users have the ability to manually create ad-hoc flights into the system via a Flight Management function in the IAM flight grid. Once created this flight is automatically added to the Gate plan Gantt chart for visualization and management.

5.6. Baggage Input Console

SITA shall work with JWA to maintain this system and ensure smooth operation.

6. Delivery Schedule

The following provide a summary of the items provided to JWA.

1. Configure Icinga Server Monitoring
2. Extend Existing Back-End Storage Infrastructure Support
3. On-Going JWA Spares Stock Replenishment
4. Business As Usual (BAU) Support And Maintenance
5. PCI-DSS Compliance Audit Support

7. Applicable Standards

7.1. SITA IPS CUSE/CUPPS

The SITA IPSCUSE software deployed at JWA will be compliant with the IATA CUPPS standard, versions 1.00, 1.01, 1.03, or latest available.

7.2. CUSS

The SITA CUSS platform is compliant to the current version of the CUSS standard as published by IATA. SITA remains current with future CUSS standards and if/when, a later standard is released, during the life of this SOW, and then an upgrade to that standard will be planned if JWA intends to operate the system past the end of support date for the current version (1.3). Upgrades are predicated on the certification of the JWA airlines.

7.3. Americans with Disability Act (ADA)

All Kiosks being proposed within this SOW will be, compliant with the current ADA legislation at the point of execution of the contract. Should any subsequent legislation require additional modifications for compliance then the impact of this will be negotiated and agreed upon with JWA.

7.4. PCI-DSS

7.4.1. Kiosk

The kiosks will form part of a PCI DSS compliant solution.

SITA will support SITA IPS Airport Systems and JWA to meet the requirements of a PCI-DSS Audit within its scope of work.

7.5 Security Audits

7.5.1 Maintain complete and accurate records such relating to systems to support JWA's audits, if any, or equivalent data protection practices and reasonably cooperate with all County reviews and testing of any solution provided by SITA IPS.

8. Task Order Process

The Task Order Process refers to the budget assigned by JWA for all items within this SOW that are not under the financial responsibility of SITA IPS. (i.e. SITA IPS will manage the task but not pay for the time or asset required).

Examples of tasks within this SOW that may require a Task Order to be raised are:

1. Out of Warranty Asset Maintenance
2. Additional PCI DSS Audit Support above allotted 25 days annually or for increased standards.

The process for a Task Order is as follows:

1. SITA IPS Site Admin / Account Manager alerts JWA to the need for a task order invoice to be raised.
2. SITA IPS raises a Task Order Invoice with a clear justification of the need and relevance to JWA
3. JWA issues a written approval (or denial) for SITA IPS to procure the Asset or expand effort as required.
4. JWA issues a payment to SITA IPS within 30 days of the Task Order Invoice date

For clarification, the Task Order budget will be managed by JWA, SITA IPS's responsibility will only be to raise Task Order Invoices as and when necessary for the continued delivery of the requirements of this SOW.

8.1. RFID Bag Tag Printers / Baggage Tags

Due to special operational requirements, Delta Air Lines positions are equipped with RFID capable bag tag printers. While these printers are backwards compatible with the non-RFID equivalents and can be used at any agent position, they require special attention. There needs to be a separate spare stock of RFID modules or pre-programmed printers for hot-swap replacements if required. The local teams (JWA Support Team and SITA Site Administrator/Local Account Manager) in accordance with agreed procedures can undertake this programming activity.

9. Contact Information

Company	Person	Function
SITA	Oleksandr Poljancyka 600 Galleria Blvd SE, Suite 1000 Atlanta, GA 30339	Account Sales Director USA Southwest Territory
SITA	Daniel Dunn 5323 Millenia Lakes Blvd. Suite 300 Orlando, FL 32839 (202) 351-9647	Senior Manager Infrastructure Management, North America
SITA	Balázs Csongrádi 5323 Millenia Lakes Blvd. Suite 300 Orlando, FL 32839 (980) 666-9019	Head of Technical Solutions, North Americas
SITA	Cliff Greenwood 5323 Millenia Lakes Blvd. Suite 300 Orlando, FL 32839 (407) 592-6046	Implementation Engineer

ATTACHMENT D
SUBCONTRACTORS

1. **Subcontractor(s)**
Listed below are subcontractor(s) anticipated by Contractor to perform services specified in Attachment A. Substitution or addition of Contractor's subcontractors in any given project function shall be allowed only with prior written approval of County's Project Manager.

Company Name & Address	Service(s)	Pricing Reference
KIS KIOSK Information Systems 356 S Arthur Avenue Louisville, CO Jake Davis (303) 661-1641	Work completed on previous amendment, remains supplier of Kiosks	As needed per JWA Approval
TSI Terminal Systems International, Inc. 2210 Hanselman Avenue Saskatoon, SK Canada S7L 6A4 Curtis Reid 306-934-6911	Providing solutions for Flight information displays throughout the airport.	Included in "Annual CUPPS/CUSS Support "core costs described in Section, 1.7, Total Summary of Pricing, Item 500.
AeroCloud Systems 1990 Main Street, Suite 801, Sarasota, FL 34236 Andrew Hope (941) 226 8215	Providing Ramp Management services for aircraft parking and information reporting on these services.	Included in "Annual CUPPS/CUSS Support "core costs described in Section, 1.7, Total Summary of Pricing, Item 500.

ATTACHMENT G
FEES & CHARGES

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

1.1 Costs for CUPPS and CUSS for Two Year Extension (Years 6 and 7)

Item	Description	Qty	Unit Price	NTE (2 Years)
Core Costs Applications and Subscriptions				
101	CUPPS & CUSS Software application support Including - Software updates and patch management - Release management - Site update support for airline applications - Fixed term support package to 5/31/2027	2	$300,899.59	$601,799.18
102	SITA FIDS/AODB/RMS system Including - Support - Fixed term subscription license to 5/31/2027	2	$185,840.46	$371,680.92
		Total One-Time Costs	**$486,740.05**	**$973,480.10**

RMS Tools				
103	Forecasting, outage and tow management -Forecast tool and future stand planning -Stand outage management and planning of outages shown within the system for scheduled closures or temporary maintenance. -Tow Management allows airport to define and readily setup tows against specific flights and allocations, using simple point and click on the Gantt Chart.	2	$30,400.12	$60,800.24
		Total RMS Options	**$30,400.12**	**$60,800.24**

Recurring Costs per year				
104	Service Management Tool	Per Year	$17,739.20	$35,478.40
105	Remote System Monitoring Tool	Per Year	$17,739.20	$35,478.40
106-1	On-Site Support Service *Including* *- Preventative Maintenance*	Per Year	Not required as SNA to continue providing	Not required as SNA to continue providing
107-2	Remote SITA help desk service *- Call receipt & dispatch 24x7* *- Monthly Reporting*	Per Year	$185,508.31	$371,016.62
108	Site Administration (2) *- Incident Management* *- Spare Management*	Per Year	$442,900.71	$885,801.42
109	3rd Level System Support for Server Environment *- Site configuration management* *- System support specialists 24x7 access*	Per Year	$177,391.96	$354,783.92
110	Documentation	Per Year	Included	Included
111	Ongoing Account Management Including - Project Management Germany & USA	Per Year	Included	Included
112	Badging Processes & Costs	Per Year	Included	Included
113	PCI Support (25 days Per annum)	Per Year	$35,478.39	$70,956.78
114	SITA 3rd Level Software Support for CUPPS Software, Licensing & Upgrades Including *- CUPPS Software* *- Software Maintenance*** *- 3rd Level Support*	Per Year	Included in #101	Included in #101
115	SITA 3rd Level Software Support for CUSS Software, Licensing & Upgrades *Including* *- CUSS Software* *- Software Maintenance*** *- 3rd Level Support*	Per Year	Included in #101	Included in #101
		Total Recurring Cost	**$876,757.77**	**$1,753,515.54**

1.1 Summary Costs for CUPPS and CUSS for Two Year Extension	
Core Costs Applications and Subscriptions	**$973,480.10**
RMS Tools	**$60,800.24**
Recurring Costs (Service)	**$1,753,515.54**
Subtotal	**$2,787,795.88**

1.2 Additional Work and Related Pricing
*** Per section 1.4 Additional Work (Must be approved by County Project Manager)**

Item	Description	Unit Price	Qty	NTE (2 Years)
200	Cybersecurity Engineer (Year 6)	$1,480.00	50 days	$74,000.00
200	Cybersecurity Engineer (Year 7)	$1,480.00	50 days	$74,000.00
	Total Additional Work			**$148,000.00**

Hourly Labor Rates

Line	Position Responsibility	Year 6	Year 7
	SITA Americas Personnel		
1	Senior Project Manager	$185.00	$189.63
2	PCI Manager	$160.00	$164.00
3	Quality Manager	$150.00	$153.75
4	Airline Integration Manager	$160.00	$164.00
5	Cybersecurity Engineer	$185.00	$189.63
	SITA HQ Support Personnel		
6	Developer	$175.00	$179.38
7	Network Engineer	$200.00	$205.00
8	Procurement	$110.00	$112.75
9	Product Management	$170.00	$174.25
10	Project Management	$155.00	$158.88
11	Quality Assurance	$155.00	$158.88
12	Service Engineer	$195.00	$199.88
13	Technical Project Management – Lead Engineer	$160.00	$164.00
14	Technical Field Advisor – Engineer	$150.00	$153.75

SUMMARY OF COSTS	**Total**	**Year 6**	**Year 7**
1.1 Core Costs Applications and Subscriptions	**$973,480.10**	**$486,740.05**	**$486,740.05**
RMS Tools	**$60,800.24**	**$30,400.12**	**$30,400.12**
Recurring Costs (Service)	**$1,753,515.54**	**$876,757.77**	**$876,757.77**
Total	***$2,787,795.88***	***1,393,897.94***	***1,393,897.94***
1.2 Additional Work and Related Pricing			
Cybersecurity Engineer Year 6	$74,000.00	$74,000.00	$0.00
Cybersecurity Engineer Year 7	$74,000.00	$0.00	$74,000.00
Additional Work Year 6 (Third Party Software/Hourly Rates)	$300,000.00	$300,000.00	
Additional Work Year 7(Third Party Software/Hourly Rates)	$300,000.00		$300,000.00
Total	***748,000.00***		
Year 6 Contract Amount Shall Not Exceed:		**1,767,897.94**	
Year 7 Contract Amount Shall Not Exceed:			**1,767,897.94**
Total Contract Amount Shall Not Exceed:	**3,535,795.88**		