COUNTY OF SONOMA

AGREEMENT BETWEEN THE COUNTY OF SONOMA AND THE ACT 1 GROUP, INC DBA ATIMS FOR JAIL MANAGEMENT SYSTEM

This Agreement is entered into by and between the County of Sonoma (the "County") and The Act 1 Group, Inc. DBA ATIMS ("Contractor") (the "Agreement") for a Jail Management System.

On **DATE**, the Board of Supervisors approved this Agreement.

The effective date of the Agreement is **DATE**. The parties, intended to be bound, mutually agree as follows:

	KEY PROVISIONS
AGREEMENT TITLE:	Jail Management System
AGREEMENT NUMBER:	**Agreement Number**
AGREEMENT TERM:	**DATE to DATE**, with County options to extend for two (2) additional 2-year periods, unless terminated earlier or otherwise amended
AUTHORIZED USER:	Office of the Sheriff
COUNTY CONTACT:	
CONTRACTOR:	The Act 1 Group, Inc. dba ATIMS 21622 Plummer Street, Suite 210 Chatsworth, CA 91311
CONTRACTOR CONTACT:	Felix Rabinovich, Vice President Email: FelixR@atims.com Phone: 818-836-6561
PURPOSE:	To establish a contract with the Contractor for a Jail Management System
TAX STATUS:	Non-Taxable

PAYMENT TERMS: Net 30

TOTAL AGREEMENT VALUE: Total Agreement Value Not to Exceed $3,290,044
Contractor acknowledges that this Not to Exceed figure does not represent a commitment by County to Contractor.

COUNTY CONTRACT ADMINISTRATOR(S):

REFERENCE/S: The following exhibits are incorporated into and constitute a material part of the Agreement. In the event of any conflict between or among the provisions contained in the Agreement, the order of precedence is as follows:

Exhibit A: County of Sonoma Standard Terms and Conditions

Exhibit B: Payment and Fee Schedule

Exhibit C: Insurance Requirements

Exhibit D: FBI CJIS Security Addendum

Exhibit E: CLETS Private Contractor Management Control Agreement

Exhibit F: CLETS Employee/Volunteer Statement

Exhibit G: Business Associate Agreement

Exhibit H: County Policy 9-2 Information Technology Use and Security Policy

Exhibit I: County Policy 9-4 Information Technology Professionals Policy

Exhibit J: County Policy 9-6 Information Technology Artificial Intelligence (AI) Policy

Exhibit K: Statement of Work

Exhibit L: ATIMS In-Custody Jail Management System (JMS) Cloud-Solution Service Level Agreement (SLA) & Support & Maintenance Agreement (“Support Agreement”)

Exhibit M: Technical Requirements

Exhibit N: Functional Requirements

Exhibit O: Interfaces

By signing below, signatory warrants and represents that he/she executed this Agreement in his/her authorized capacity, that he/she has the authority to bind the entity listed below to contractual obligations and that by his/her signature on this Agreement, the entity on behalf of which he/she acted, executed this Agreement.

COUNTY OF SONOMA

_____
Date

CONTRACTOR

Signature: _____

Print: Felix Rabinovich

Title: Vice President

Date: _____

Signed and certified that a copy of this
document has been delivered by electronic
or other means to the President, Board of Supervisors.

ATTEST:

_____
Date

APPROVED AS TO FORM AND LEGALITY

_____
Date

Exhibit A
County of Sonoma Standard Terms and Conditions

DEFINITIONS

a. "County Confidential Information" shall include all material, non-public information (including material, non-public County Data) appearing in any form (including, without limitation, written, oral or displayed), that is disclosed, directly or indirectly, through any means of communication by County, its agents or employees, to Contractor, its agents or employees, or any of its affiliates or representatives.
b. "County Data" shall mean data and information received by Contractor from County. County Data includes any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a contractor for use by County. As between Contractor and County, all County Data shall remain the property of County.
c. "Deliverables" means goods, services, software, hardware, information technology, telecommunications technology, enhancements, updates, new versions or releases, documentation, and any other items to be delivered pursuant to this Agreement, including any such items furnished incident to the provision of services.
d. "Documentation" means manuals and other printed materials (including updates and revisions) necessary or useful to the County in its use or maintenance of the Deliverables provided pursuant to this Agreement.
e. When used in this Agreement, "days" shall refer to calendar days unless stated otherwise.

1. NON-EXCLUSIVE AGREEMENT

The Agreement does not establish an exclusive contract between the County and the Contractor. The County expressly reserves rights to, without limitation, the following: the right to utilize others to provide products, support and services; the right to request proposals from others with or without requesting proposals from the Contractor; and the unrestricted right to bid any such product, support or service.

2. DELIVERABLES

Contractor agrees to provide the County all Deliverables on terms set forth in the Agreement, including all Exhibits that are attached to the Agreement and incorporated, as well as all necessary equipment and resources. However, this Agreement does not provide authority to ship Deliverables. That authority shall be established by contract release purchase orders placed by the County and sent to Contractor throughout the term of the Agreement. Each and every contract release purchase order shall incorporate all terms of this Agreement and this Agreement shall apply to same.

Any additional or different terms or qualifications sent by Contractor, including, without limitation, electronically or in mailings, attached to invoices or with any deliverables shipped, shall not become part of the contract between the parties. County's acceptance of Contractor's offer is expressly made conditional on this statement.
Contractor shall timely provide to the County, all documentation and manuals relevant to the Deliverables to be supplied, at no additional cost. Such documentation shall be delivered either in advance of the delivery of Deliverables or concurrently with the delivery of Deliverables.

Employees and agents of Contractor, shall, while on the premises of the County, comply with all rules and regulations of the premises, including, but not limited to, security requirements. If required, Contractor shall be responsible for installation, training and knowledge transfer activities in relation to the Deliverables being supplied.

All equipment shall be delivered to a County site specified in the contract release purchase order, or if not so specified therein, in the Statement of Work (SOW)/Specifications.

Contractor holds itself out as an expert in the subject matter of the Agreement. Contractor represents itself as being possessed of greater knowledge and skill in this area than the average person. Accordingly, Contractor is under a duty to exercise a skill greater than that of an ordinary person, and the manner in which performance is rendered will be evaluated in light of the Contractor's superior skill. Contractor shall provide equipment and perform work in a professional manner consistent, at minimum, with industry standards.

Contractor represents that all prices, warranties, benefits and other terms being provided hereunder are fair, reasonable and commensurate with the terms otherwise being offered by Contractor to its current customers

ordering comparable Deliverables and services. County does not guarantee any minimum orders.

3. NECESSARY ACTS AND FURTHER ASSURANCES

The Contractor shall at its own cost and expense execute and deliver such further documents and instruments and shall take such other actions as may be reasonably required or appropriate to evidence or carry out the intent and purposes of this Agreement.

4. COUNTING DAYS

Days are to be counted by excluding the first day and including the last day, unless the last day is a Saturday, a Sunday, or a legal holiday, and then it is to be excluded.

5. PRICING

Unless otherwise stated, prices shall be fixed for the term of the Agreement, including all extensions. If any product listed in this Agreement is discontinued or upgraded prior to delivery, Contractor shall extend the same pricing towards a comparable replacement which is functionally equivalent or an upgraded version.

Exhibit B of the Agreement is the basis for pricing and compensation throughout the term of the Agreement.

Notwithstanding the above, if at any time during the term of the Agreement the Contractor offers special, promotional or reduced pricing when compared with the price paid by the County, County shall benefit from that pricing, and that pricing shall apply to the County at the same time that is offered to other entities. Contractor is required, on an ongoing basis, to inform the County of any such special, promotional or reduced pricing.

6. MODIFICATION

This Agreement or any contract release purchase order may be supplemented, amended, or modified only by the mutual agreement of the parties. No supplement, amendment, or modification of this Agreement contract release purchase order will be binding on County unless it is in writing and signed by the County's authorized representative.

7. TIME OF THE ESSENCE

Time is of the essence in the delivery of goods by Contractor under this Agreement and any contract release purchase order. If Contractor fails to deliver goods and/or services on time, the Contractor shall be liable for any costs incurred by the County proximately caused by Contractor's delay. For instance, County may purchase or obtain the goods and/or services elsewhere and the Contractor shall be liable for the difference between the price in the Agreement and the cost to the County; or to the extent such delay is not caused in substantial part or in full by County, County may terminate on grounds of material breach and Contractor shall be liable for County's damages proximately caused by Contractor's failure to deliver.

The Contractor shall promptly reimburse the County for the full amount of its liability based on the preceding paragraph, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract with the County.

The rights and remedies of County provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law. The acceptance by County of late or partial performance with or without objection or reservation shall not waive the right to claim damage for such breach nor constitute a waiver of the rights or requirements for the complete and timely performance of any obligation remaining to be performed by the Contractor, or of any other claim, right or remedy of the County.

8. HAZARDOUS SUBSTANCES

If any product being offered, delivered or supplied to the County is listed in the Hazardous Substances List of the Regulations of the Director of Industrial Relations with the California Occupational Safety and Health Standards Board, or if the product presents a physical or health hazard as defined in the California Code of Regulations, General Industry Safety Order, Section 5194 (T8CCR), Hazard Communication, the Contractor must include a Material Safety Data Sheet (MSDS) with delivery, or shipment. Each MSDS must reference the contract/purchase order number, and identify the "Ship To Address". All shipments and containers must comply with the labeling requirements of Title 49, Code of Federal Regulations by identifying the hazardous substance, name and address

of manufacturer, and appropriate hazard warning regarding potential physical safety and health hazard.

9. SHIPPING AND RISK OF LOSS

Goods shall be packaged, marked and otherwise prepared by Contractor in suitable containers in accordance with sound commercial practices. Contractor shall include an itemized packing list with each shipment and with each individual box or package shipped to the County. The packing list shall contain, without limitation, the applicable contract release purchase order number.

Unless otherwise specified in writing, all shipments by Contractor to County will be F.O.B. point of destination. Freight or handling charges are not billable unless such charges are referenced on the order. Transportation receipts, if required by contract release purchase order, must accompany invoice. Regardless of F.O.B. point, Contractor agrees to bear all risks of loss, injury, or destruction to goods and materials ordered herein which occur prior to delivery at County's destination; and such loss, injury or destruction shall not release Contractor from any obligation hereunder.

Any shipments returned to the Contractor shall be delivered as F.O.B. shipping point.

10. INSPECTION AND RELATED RIGHTS

All goods and services are subject to inspection, testing, approval and acceptance by the County. Inspection shall be made within 60 days or a reasonable time after delivery, whichever period is longer.

If the goods, services, or the tender of delivery fail in any respect to conform to the contract, the County may reject the entire tender, accept the entire tender, or, if the deliverables are commercially divisible, may, at its option, accept any commercial unit or units and reject the rest.

Contractor shall be responsible to reclaim and remove any rejected goods or items at its own expense. Should Contractor fail to reclaim or remove any rejected goods or items within a reasonable time, County shall, at its option dispose of such goods or items and require reimbursement from Contractor for any costs or expenses incurred.

In the event that the Contractor's goods are not accepted by County, the Contractor shall be liable for any costs incurred by the County proximately caused by such failure by Contractor. For instance, County may purchase or obtain the goods elsewhere and the Contractor shall be liable for the difference between the price in the Agreement and the cost to the County, and any other direct costs incurred; or County may terminate for cause on grounds of material breach and Contractor shall be liable for County's direct damages proximately caused by Contractor's failure to perform.

The Contractor shall promptly reimburse the County for the full amount of its liability based on the preceding paragraph, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract with the County.

The rights and remedies of County provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law. The acceptance by County of late or partial performance with or without objection or reservation shall not waive the right to claim damage for such breach nor constitute a waiver of the rights or requirements for the complete and timely performance of any obligation remaining to be performed by the Contractor, or of any other claim, right or remedy of the County.

11. ADJUSTMENT BY COUNTY

The County reserves the right to waive a variation in specification of goods or services supplied by the Contractor. Contractor may request an equitable adjustment of payments to be made by County if County requires a change in the goods or services to be delivered. Any claim by the Contractor for resulting adjustment of payment must be asserted within 30 days from the date of receipt by the Contractor of the notification of change required by County; provided however, that the County's authorized representative decides that the facts justify such action, may receive and act upon any such claim asserted at any time prior to final payment made for goods and services supplied by Contractor. Where the cost of property made obsolete or excess as a result of a change is included in the Contractor's claim for adjustment, the County's authorized representative shall have the right to prescribe the manner of disposition of such property. Nothing in this clause shall excuse performance by Contractor.

12. INVOICING

Contractor shall invoice according to Exhibit B of the Agreement. Invoices shall be sent to the County customer or department referenced in the individual contract release purchase order. Invoices for goods or services not specifically listed in the Agreement will not be approved for payment.

Invoices shall include: Contractor's complete name and remit-to address; invoice date, invoice number, and payment term; County contract number; pricing per the Agreement; applicable taxes; and total cost.

Contractor and County shall make reasonable efforts to resolve all invoicing disputes within seven (7) days.

13. PAYMENT

The County's standard payment term shall be Net thirty (30), unless otherwise agreed to by the parties. Payment shall be due Net Thirty (30) days from the date of receipt and approval of correct and proper invoices.

Payment is deemed to have been made on the date the County mails the warrant or initiates the electronic fund transfer.

14. OTHER PAYMENT PROVISIONS

Notwithstanding anything to the contrary, County shall not make payments prior to receipt of service or goods (i.e. the County will not make "advance payments"). Unless specified in writing in an individual purchase order, the County will not accept partial delivery with respect to any purchase order. Any acceptance of partial delivery shall not waive any of County's rights on an ongoing basis.

Sales tax shall be noted separately on every invoice. Items that are not subject to sales tax shall be clearly identified.
Contractor shall be responsible for payment of all state and federal taxes assessed on the compensation received under this Purchase Order and such payment shall be identified under the Contractor's federal and state identification number(s).

The County does not pay Federal Excise Taxes (F.E.T). The County will furnish an exemption certificate in lieu of paying F.E.T. Federal registration for such transactions is: County #94730482K. Contractor shall not charge County for delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, cost of bonds, or for any other purpose, unless expressly authorized by the County.

15. LATE PAYMENT CHARGES OR FEES

The Contractor acknowledges and agrees that the County will not pay late payment charges.

16. DISALLOWANCE

In the event the Contractor receives payment for goods or services, which payment is later disallowed by the County or state or federal law or regulation, the Contractor shall promptly refund the disallowed amount to the County upon notification. At County's option, the County may offset the amount disallowed from any payment due to the Contractor under any contract with the County.

17. TERMINATION FOR CONVENIENCE

The County may terminate this Agreement or any order at any time for the convenience of the County, specifying the effective date and scope of such termination.

In no event shall the County be liable for costs incurred by the Contractor as a result of the termination or any loss of profits on the resulting order or portion thereof so terminated. In the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other materials (collectively referred to as "materials") prepared by Contractor under this Agreement contract release purchase order shall become the property of the County, and shall be promptly delivered to the County. Upon receipt of such materials, County shall pay the Contractor as full compensation for performance, the unit or pro rata price for the then-accepted portion of goods and/or services. If this Agreement is terminated, neither party may nullify obligations, if any, already incurred prior to the date of termination.

Termination for Convenience may be exercised any time by and at the sole discretion of the County.

18. TERMINATION FOR CAUSE

County may terminate this Agreement or any order, in whole or in part, for cause upon thirty (30) days written notice to Contractor. For purposes of this Agreement, cause includes, but is not limited to, any of the following: (a) material breach of this Agreement or any contract release purchase order by Contractor, (b) violation by Contractor of any applicable laws or regulations; (c) assignment or delegation by Contractor of the rights or duties under this Agreement without the written consent of County or (d) less than perfect tender of delivery or performance by Contractor that is not in strict conformance with terms, conditions, specifications, covenants, representations, warranties or requirements in this Agreement or any order.

In the event County terminates for cause under this provision, the Contractor shall be liable for any costs incurred by the County to the extent proximately caused by Contractor's default. The Contractor shall promptly reimburse the County for the full amount of its liability determined under this paragraph, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract or order with the County.

If, after notice of termination under the provisions of this clause, it is determined for any reason that the Contractor was not in default under this provision of this clause, the County has the option to make its notice of termination pursuant to the Termination for Convenience clause and the rights and obligations of the parties would be in accordance with that provision.

In lieu of terminating immediately upon contractor's default, County may, at its option, provide written notice specifying the cause for termination and allow Contractor ten (10) days (or other specified time period by the County) to cure. If, within ten (10) days (or other specified time) after the County has given the Contractor such notice, Contractor has not cured to the satisfaction of the County, or if the default cannot be reasonably cured within that time period, County may terminate this Agreement at any time thereafter. County shall determine whether Contractor's actions constitute complete or partial cure. In the event of partial cure, County may, at its option, decide whether to (a) give Contractor additional time to cure while retaining the right to immediately terminate at any point thereafter for cause; or (b) terminate immediately for cause. If this Agreement is terminated, neither party may nullify obligations, if any, already incurred prior to the date of termination.

Notwithstanding any of the above, if County determines that any action by Contractor contributes to the curtailment of an essential service or pose an immediate threat to life, health, or property, County may terminate this Agreement effective immediately without penalty or opportunity to cure upon issuing either oral or written notice to the Contractor.

IMMEDIATE TERMINATION FOR CAUSE

Notwithstanding any other provision in this Agreement:

(1) Contractor's failure to comply with all terms and conditions set forth in Section 63 (Information Security Compliance), Exhibit D (FBI CJIS Security Addendum), Exhibit E (CLETS Private Contractor Management Control Agreement), Exhibit I (County Information Technology User Responsibility Statement for Third Parties), and Exhibit H (Vendor Remote Access Statement), or failure to require such compliance of its officers, employees, contractors, subcontractors, and agents ("Contractor's personnel") engaged in performance of this Agreement, shall constitute a material breach of this Agreement and the County may immediately terminate this Agreement for cause.

(2) Contractor shall not allow Contractor's personnel to perform services for the County unless and until its employees sign Exhibit D (FBI CJIS Security Addendum), Exhibit F (CLETS Employee Volunteer Statement), Exhibit I (County Information Technology User Responsibility Statement for Third Parties), and Exhibit H (Vendor Remote Access Statement). If Contractor's personnel access County Data or County systems without first signing, that will constitute a material breach of this Agreement and the County may immediately terminate this Agreement for cause.

(3) Contractor shall monitor the compliance of Contractor's personnel with the terms in Section 63, Exhibit D (FBI CJIS Security Addendum), Exhibit E (CLETS Private Contractor Management Control Agreement), Exhibit F (CLETS Employee Volunteer Statement), Exhibit I (County Information Technology User Responsibility Statement for Third Parties), and Exhibit H (Vendor Remote Access Statement), and shall notify County no later than 24 hours after Contractor discovers any violations. Contractor's failure to monitor Contractor's personnel or timely notify the County shall constitute a material breach of this

Agreement, and the County may immediately terminate this Agreement for cause.

In the event of Immediate Termination for Cause, the rights and obligations in Section 18 (Termination for Cause) apply, except for the thirty (30) day notice period and ten (10) day cure period.

19. TERMINATION FOR BANKRUPTCY

If Contractor is adjudged to be bankrupt or should have a general assignment for the benefit of its creditors, or if a receiver should be appointed on account of Contractor's insolvency, the County may terminate this Agreement immediately without penalty. For the purpose of this Section, bankruptcy shall mean the filing of a voluntary or involuntary petition of bankruptcy or similar relief from creditors; insolvency; the appointment of a trustee or receiver, or any similar occurrence reasonably indicating an imminent inability to perform substantially all the party's duties under this Agreement. If this Agreement is terminated, neither party may nullify obligations, if any, already incurred prior to the date of termination.

20. BUDGETARY CONTINGENCY

Performance and/or payment by the County pursuant to this Agreement is contingent upon the appropriation by the County of sufficient funds for Deliverables covered by this Agreement. If funding is reduced or deleted by the County for services covered by this Agreement, the County may, at its option and without penalty or liability, terminate this Agreement or offer an amendment to this Agreement indicating the reduced amount.

21. DISENTANGLEMENT

Contractor shall cooperate with County and County's other contractors to ensure a smooth transition at the time of termination of this Agreement, regardless of the nature or timing of the termination. Contractor shall cooperate with County's efforts to ensure that there is no interruption of work required under the Agreement and no adverse impact on the supply of goods, provision of County services or the County activities. Contractor shall return to County all County assets or information in Contractor's possession.

For any software programs developed for use under the County's Agreement, Contractor shall provide a nonexclusive, nontransferable, fully-paid, perpetual, irrevocable, royalty-free worldwide license to the County, at no charge to County, to use, copy, and modify, all work or derivatives that would be needed in order to allow County to continue to perform for itself, or obtain from other providers, the services as the same might exist at the time of termination.

Contractor shall promptly remove from County's premises, or the site of the work being performed by Contractor for County, any Contractor assets that County, or its designee, chooses not to purchase under this provision.

Contractor shall deliver to County or its designee, at County's request, all documentation and data related to County, including, but not limited to, the County Data and client files, held by Contractor, within sixty (60) days of the request, and after return of same, Contractor shall destroy all copies thereof not turned over to County, all at no charge to County.

22. DISPUTES

Except as otherwise provided in this Agreement, any dispute arising under this contract that is not disposed of by Agreement shall be decided by the County's authorized representative or designee, who shall furnish the decision to the Contractor in writing. The decision of the County's authorized representative or designee shall be final and conclusive. The Contractor shall proceed diligently with the performance of the Agreement pending the County's authorized representative or designee's decision. The County's authorized representative or designee shall not be required to decide issues that are legal or beyond his or her scope of expertise.

23. ACCOUNTABILITY

(1) Contractor will be the primary point of contact regarding the Deliverables, including performance thereof, for subcontractors approved by the County under this Agreement including all exhibits hereunder.

(2) Contractor shall enter into all contracts with approved subcontractors necessary to perform the services under this Agreement prior to the execution of this Agreement.

(3) Any work performed by a subcontractor shall be considered work performed by Contractor. Contractor shall be responsible and liable for any action or inaction of subcontractors, and for ensuring that all subcontractors comply with the Agreement.

(4) As between Contractor and any subcontractors, Contractor shall assume the responsibility under this Agreement for (i) of all matters relating to the County's purchase of the Deliverables and (ii) Contractor's performance of all obligations for provisions of the Deliverables, including performance by all subcontractors. If issues regarding Contractor's or any subcontractor's performance under this Agreement arise, the Contractor must take immediate corrective action pursuant to this Agreement.

(5) Contractor shall inform all subcontractors of all obligations related to the provision and performance of Deliverables under the Agreement, including all exhibits, and obtain subcontractor's written acknowledgment of such obligations. By way of example and not limitation, Contractor shall ensure that all subcontractors are subject to its obligations protecting and limiting the use and disclosure of County Confidential Information and County Data.

(6) Nothing in this Agreement relieves subcontractors of their obligations under this Agreement.

24. NO ASSIGNMENT, DELEGATION OR SUBCONTRACTING WITHOUT PRIOR WRITTEN CONSENT

Contractor may not assign any of its rights, delegate any of its duties or subcontract any portion of its work or business under this Agreement or any contract release purchase order without the prior written consent of County. No assignment, delegation or subcontracting will release Contractor from any of its obligations or alter any of its obligations to be performed under the Agreement. Any attempted assignment, delegation or subcontracting in violation of this provision is voidable at the option of the County and constitutes material breach by Contractor. As used in this provision, "assignment" and "delegation" means any sale, gift, pledge, hypothecation, encumbrance, or other transfer of all or any portion of the rights, obligations, or liabilities in or arising from this Agreement to any person or entity, whether by operation of law or otherwise, and regardless of the legal form of the transaction in which the attempted transfer occurs.

25. MERGER AND ACQUISITION

The terms of this Agreement will survive an acquisition, merger, divestiture or other transfer of rights involving Contractor. In the event of an acquisition, merger, divestiture or other transfer of rights Contractor must ensure that the acquiring entity or the new entity is legally required to:

(1) Honor all the terms negotiated in this Agreement and any pre-acquisition or pre-merger Agreement between Contractor and the County, including but not limited to a) established pricing and fees; b) guaranteed product support until the contract term even if a new product is released; and c) no price escalation during the term of the Agreement.

(2) If applicable, provide the functionality of the products provided hereunder, including the software as a service, in a future, separate or renamed product, if the acquiring entity or the new entity reduces or replaces the functionality, or otherwise provide a substantially similar functionality of the current licensed product. The County will not be required to pay any additional license or maintenance fee to an acquiring entity in order to continue with full use, benefit, and functionality of the products provided hereunder, including the software as a service provided under this Agreement until expiration or termination.

(3) Give 30-days written notice to the County following the closing of an acquisition, merger, divestiture or other transfer of right involving Contractor.

26. COMPLIANCE WITH ALL LAWS & REGULATIONS APPLICABLE TO GOODS AND/OR SERVICES PROVIDED

Contractor shall comply with all laws, codes, regulations, rules and orders (collectively, "Regulations") applicable to the goods and/or services to be provided hereunder. Contractor's violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the contract. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 *et seq*. the Fair Packaging and Labeling Act, and the standards and regulations issued there under. Contractor agrees to indemnify and hold harmless the County for any loss, damage, fine, penalty, or any expense whatsoever as a result of Contractor's failure to comply with any Regulation applicable to the goods and/or services to be provided

hereunder.

27. FORCE MAJEURE

Neither party shall be liable for failure of performance, nor incur any liability to the other party on account of any loss or damage resulting from any delay or failure to perform all or any part of this Agreement if such delay or failure is caused by events, occurrences, or causes beyond the reasonable control and without negligence of the parties. Such events, occurrences, or causes will include acts of God/nature (including fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, riots, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, lockout, blockage, embargo, labor dispute, strike, interruption or failure of electricity or telecommunication service ("Force Majeure Event").

Each party, as applicable, shall give the other party notice of its inability to perform and reasonable detail of the cause of the inability. Each party must use best efforts to remedy the situation and remove, as soon as practicable, the cause of its inability to perform or comply.

The party asserting a Force Majeure Event as a cause for non-performance shall have the burden of proving that reasonable steps were taken to minimize delay or damages caused by foreseeable events, that all non-excused obligations were substantially fulfilled, and that the other party was timely notified of the likelihood or actual occurrence which would justify such an assertion, so that other prudent precautions could be contemplated.

The County shall reserve the right to terminate this Agreement and/or any applicable order or contract release purchase order effective immediately, upon written notice, in the event of non-performance by Contractor because of a Force Majeure Event. The County shall reserve the right to extend the agreement and time for performance at its discretion.

28. INDEPENDENT CONTRACTOR

Contractor shall supply all goods and/or perform all services pursuant to this Agreement as an independent contractor and not as an officer, agent, or employee of County. Contractor shall be solely responsible for the acts, and omissions of its officers, agents, employees, contractors, and subcontractors, if any. Nothing herein shall be considered as creating a partnership or joint venture between the County and Contractor. No person performing any services and/or supplying all goods shall be considered an officer, agent, or employee of County, nor shall any such person be entitled to any benefits available or granted solely to employees of the County.

Contractor is responsible for payment to sub-contractors and must monitor, evaluate, and account for the sub-contractor(s) services and operations.

29. INSURANCE

Contractor shall maintain insurance coverage pursuant to the exhibit setting forth insurance requirements if such exhibit is attached to the Agreement.

30. DAMAGE AND REPAIR BY CONTRACTOR

Any and all damages to County owned or leased property caused by Contractor's negligence or operations shall be repaired, replaced or reimbursed by Contractor at no charge to the County. Repairs and replacements shall be completed within seventy-two (72) hours of the incident unless the County requests or agrees to an extension or another time frame. Contractor must immediately report each incident to the County's Director of Procurement or designee. Damage observed by Contractor, whether or not resulting from Contractor's operations or negligence shall be promptly reported by Contractor to County. County may, at its option, approve and/or dictate the actions that are in County's best interests.

31. LIENS, CLAIMS, ENCUMBRANCES AND TITLE

The Contractor represents and warrants that all the goods and materials ordered and delivered are free and clear of all liens, claims or encumbrances of any kind. Title to the material and supplies purchased shall pass directly from Contractor to County at the F.O.B. point, subject to the right of County to reject upon inspection.

32. ASSIGNMENT OF CLAYTON ACT, CARTWRIGHT ACT CLAIMS

Contractor hereby assigns to the County all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the Contractor for sale to the County pursuant to this Agreement.

33. INDEMNITY

Contractor shall indemnify, defend, and hold harmless the County, its officers, agents and employees from any third-party claim, liability, loss, injury or damage arising out of, or in connection with, performance of this Agreement by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the sole negligence or willful misconduct of personnel employed by the County. It is the intent of the parties to this Agreement to provide the broadest possible coverage for the County. Contractor shall reimburse the County for all costs, attorneys' fees, expenses and liabilities incurred with respect to any litigation in which Contractor contests its obligation to indemnify, defend and/or hold harmless the County under this Agreement and does not prevail in that contest.

34. LIMITATION OF LIABILITY

Contractor's maximum liability to County relating to or arising from this Agreement shall not exceed USD $5,000,000 (Five Million United States Dollars) ("Limitation of Liability"). This Limitation of Liability amount shall not apply to any liability caused by Contractor's gross negligence or willful misconduct or to any of Contractor's indemnity obligations under this Agreement for third-party claims.

To the maximum extent permitted by applicable law and despite anything to the contrary in the Agreement, neither County nor Contractor shall have any liability to the other for any indirect, consequential, special, or incidental damages, damages for loss of profits or revenues relating to or arising from the services or products provided under this Agreement.

35. INTELLECTUAL PROPERTY INDEMNITY

Contractor represents and warrants for the benefit of the County and its users that it is the exclusive owner of all rights, title and interest in the product or services to be supplied.

Contractor shall, at its own expense, indemnify, defend, settle, and hold harmless the County and its employees, agents and assigns against any claim or potential claim that any good, (including software) and/or service, or County's use of any good (including software) and/or service, provided under this Agreement infringes any patent, trademark, copyright or other proprietary rights, including trade secret rights. Contractor shall pay all costs, damages and attorneys' fees that a court or other adjudicatory body awards as a result of any such claim.

36. WARRANTY

Any goods and/or services furnished under this Agreement shall be covered by the most favorable commercial warranties that Contractor gives to any of its customers for the same or substantially similar goods and/or services. Any warranties so provided shall supplement, and shall not limit or reduce, any rights afforded to County by any clause in this Agreement, any applicable Uniform Commercial Code warranties, including, without limitation, Implied Warranty of Merchantability and Implied Warranty of Fitness for a Particular Purpose as well as any other express warranty. Despite the foregoing, any support and maintenance agreement(s) between the parties shall prevail over this section in the event of a conflict among such provisions.
Contractor expressly warrants that all goods supplied shall be new, suitable for the use intended, of the grade and quality specified, free from all defects in design, material and workmanship, in conformance with all samples, drawings, descriptions and specifications furnished by the County, in compliance with all applicable federal, state and local laws and regulations and free of liens, claims and encumbrances. Contractor warrants that all services shall strictly conform to the County's requirements.

Contractor shall immediately replace or repair any good not conforming to any warranty, or provide services to conform to County's requirements. If after notice, Contractor fails to repair or replace goods, or to provide services to conform to County's requirements, Contractor shall promptly refund to County the portion of the purchase price paid by the County that is allocated to the non-conformance. This remedy is nonexclusive of other remedies and rights that may be exercised by the County. Claims for damages may include direct damages.

During the provision of goods and services, Contractor may not disclaim any warranty, express or implied, and any such disclaimer shall be void. Additionally, the warranties above shall not be deemed to exclude Contractor's standard warranties or other rights and warranties that the County may have or obtain.

37. COOPERATION WITH REVIEW

Contractor shall cooperate with County's periodic review of Contractor's performance.

Contractor shall make itself available onsite to review the progress of the project and Agreement, as requested by the County, upon reasonable advanced notice.
Contractor agrees to extend to the County or his/her designees and/or designated auditor of the County, the right to monitor or otherwise evaluate all work performed and all records, including service records and procedures to assure that the project is achieving its purpose, that all applicable County, State, and Federal regulations are met, and that adequate internal fiscal controls are maintained.

38. AUDIT RIGHTS

Pursuant to California Government Code Section 8546.7, the parties acknowledge and agree that every contract involving the expenditure of public funds in excess of $10,000 may be subject to audit by the State Auditor.

All payments made under this Agreement shall be subject to an audit at County's option, and shall be adjusted in accordance with said audit. Adjustments that are found necessary as a result of auditing may be made from current billings.

The Contractor shall be responsible for receiving, replying to, and complying with any payment adjustments set forth in any County audits. The Contractor shall pay to County the full amount determined to be due as a result of a County audit. This provision is in addition to other inspection and access rights specified in this Agreement.

39. ACCESS AND RETENTION OF RECORDS AND PROVISION OF REPORTS

Contractor shall maintain financial records adequate to show that County funds paid were used for purposes consistent with the terms of the contract between Contractor and County. Records shall be maintained during the term of the Agreement and for a period of four (4) years from its termination, or until all claims have been resolved, whichever period is longer, unless a longer period is required under any contract or applicable law.

All books, records, reports, and accounts maintained pursuant to the Agreement, or related to the Contractor's activities under the Agreement, shall be open to inspection, examination, and audit by County, federal and state regulatory agencies, and to parties whose Agreements with the County require such access. County shall have the right to obtain copies of any and all of the books and records maintained pursuant to the Agreement, upon the payment of reasonable charges for the copying of such records.

Contractor shall provide annual reports that include, at a minimum, (i) the total contract release purchase order value for the County as a whole and individual County departments, and (ii) the number of orders placed, the breakdown (by customer ID/department and County) of the quantity and dollar amount of each product and/or service ordered per year. Annual reports must be made available no later than 30 days of the contract anniversary date unless otherwise requested.

Contractor shall also provide quarterly reports to the County that show a breakdown by contract release purchase order (i) the order date (ii) ship date (iii) estimated arrival date (iv) actual arrival date (v) list of products, services and maintenance items and (vi) the number and details of problem/service calls and department name that each such call pertains to (including unresolved problems). Quarterly reports must be made available to the County in electronic format, two (2) business days after the end of each quarter unless otherwise requested.

40. ACCESS TO BOOKS AND RECORDS PURSUANT TO THE SOCIAL SECURITY ACT

Access to Books and Records: If and to the extent that, Section 1861 (v) (1) (1) of the Social Security Act (42 U.S.C. Section 1395x (v) (1) (1) is applicable, Contractor shall maintain such records and provide such information to County, to any payor which contracts with County and to applicable state and federal regulatory agencies, and shall permit such entities and agencies, at all reasonable times upon request, to access books, records and other papers relating to the Agreement hereunder, as may be required by applicable federal, state and local laws, regulations and ordinances. Contractor agrees to retain such books, records and information for a

period of at least four (4) years from and after the termination of this Agreement. Furthermore, if Contractor carries out any of its duties hereunder, with a value or cost of Ten Thousand Dollars ($10,000) or more over a twelve (12) month period, through a subcontract with a related organization, such subcontract shall contain these same requirements. This provision shall survive the termination of this Agreement regardless of the reason for the termination.

41. COUNTY NO-SMOKING POLICY

Contractor and its employees, agents and subcontractors, shall comply with the County's No Smoking Policy, as set forth in the Board of Supervisors Policy Manual section 3.47 (as amended from time to time), which prohibits smoking: (1) at the Sonoma County Sheriff's Office and all County-owned and operated health facilities, (2) within thirty (30) feet surrounding County-owned buildings and leased buildings where the County is the sole occupant, and (3) in all County vehicles.

42. FOOD AND BEVERAGE STANDARDS

Except in the event of an emergency or medical necessity, the following nutritional standards shall apply to any foods and/or beverages purchased by Contractor with County funds for County-sponsored meetings or events.

If food is to be provided, healthier food options shall be offered. "Healthier food options" include (1) fruits, vegetables, whole grains, and low fat and low calorie foods; (2) minimally processed foods without added sugar and with low sodium; (3) foods prepared using healthy cooking techniques; and
(4) foods with less than 0.5 grams of trans fat per serving. Whenever possible, Contractor shall (1) offer seasonal and local produce; (2) serve fruit instead of sugary, high calorie desserts; (3) attempt to accommodate special, dietary and cultural needs; and (4) post nutritional information and/or a list of ingredients for items served. If meals are to be provided, a vegetarian option shall be provided, and the Contractor should consider providing a vegan option. If pre-packaged snack foods are provided, the items shall contain: (1) no more than 35% of calories from fat, unless the snack food items consist solely of nuts or seeds; (2) no more than 10% of calories from saturated fat; (3) zero trans-fat; (4) no more than 35% of total weight from sugar and caloric sweeteners, except for fruits and vegetables with no added sweeteners or fats; and (5) no more than 360 mg of sodium per serving.

If beverages are to be provided, beverages that meet the County's nutritional criteria are (1) water with no caloric sweeteners; (2) unsweetened coffee or tea, provided that sugar and sugar substitutes may be provided as condiments; (3) unsweetened, unflavored, reduced fat (either nonfat or 1% low fat) dairy milk; (4) plant-derived milk (e.g., soy milk, rice milk, and almond milk) with no more than 130 calories per 8 ounce serving; (5) 100% fruit or vegetable juice (limited to a maximum of 8 ounces per container); and (6) other low-calorie beverages (including tea and/or diet soda) that do not exceed 40 calories per 8 ounce serving. Sugar-sweetened beverages shall not be provided.

43. DEBARMENT

Contractor represents and warrants that it, its employees, contractors, subcontractors or agents (collectively "Contractor") are not suspended, debarred, excluded, or ineligible for participation in Medicare, Medi-Cal or any other federal or state funded health care program, if applicable, or from receiving Federal funds as listed in the List of Parties Excluded from Federal Procurement or Non- procurement Programs issued by the Federal General Services Administration.

Contractor must within thirty (30) calendar days advise the County if, during the term of this Agreement, Contractor becomes suspended, debarred, excluded or ineligible for participation in Medicare, Medi- Cal or any other federal or state funded health care program, as defined by 42. U.S.C. 1320a-7b (f), or from receiving Federal funds as listed in the List of Parties Excluded from Federal Procurement or Non- procurement Programs issued by the Federal General Services Administration. Contractor will indemnify, defend and hold the County harmless for any loss or damage resulting from the conviction, debarment, exclusion or ineligibility of the Contractor.

44. CALIFORNIA PUBLIC RECORDS ACT

The County is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If Contractor's proprietary information is contained in documents or information submitted to County, and Contractor claims that such information falls within one or more CPRA exemptions, Contractor must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the County will make best efforts to provide notice to

Contractor prior to such disclosure. If Contractor contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Sonoma County before the County is required to respond to the CPRA request. If Contractor fails to obtain such remedy within the time the County is required to respond to the CPRA request, County may disclose the requested information.

Contractor further agrees that it shall defend, indemnify and hold County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorney's fees) that may result from denial by County of a CPRA request for information arising from any representation, or any action (or inaction), by the Contractor.

45. CONFLICT OF INTEREST; POLITICAL REFORM ACT DISCLOSURE REQUIREMENT

If applicable, Contractor shall comply with all applicable requirements governing avoidance of impermissible client conflicts; and federal, state and local conflict of interest laws and regulations including, without limitation, California Government Code section 1090 *et seq*., the California Political Reform Act (California Government Code section 87100 *et seq*.) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 *et seq*.). Failure to do so constitutes a material breach of this Agreement and is grounds for immediate termination of this Agreement by the County.

In accepting this Agreement, Contractor covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of this Agreement. Contractor further covenants that, in the performance of this Agreement, it will not use any contractor or employ any person having such an interest. Contractor, including but not limited to contractor's employees, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under this Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

Contractor, including but not limited to contractor's employees and subcontractors, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under the Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

If the disclosure provisions of the Act are applicable to any individual providing service under the Agreement, Contractor shall, upon execution of the Agreement, provide the County with the names, description of individual duties to be performed, and email addresses of all individuals, including but not limited to Contractor's employees, agents and subcontractors, that could be substantively involved in "making a governmental decision" or "serving in a staff capacity and in that capacity participating in making governmental decisions or performing duties that would be performed by an individual in a designated position," as part of Contractor's service to the County under the Agreement. Contractor shall ensure that such individuals file Statements of Economic Interests within 30 days of commencing service under the Contract, annually by April 1, and within 30 days of their termination of service under the Contract.

46. SEVERABILITY

Should any part of this Agreement between County and the Contractor or any individual contract release purchase order be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect the validity of the remainder of the Agreement or any individual contract release purchase order which shall continue in full force and effect, provided that such remainder can, absent the excised portion, be reasonably interpreted to give the effect to the intentions of the parties.

47. NON-WAIVER

No waiver of a breach, failure of any condition, or any right or remedy contained in or granted by the provisions of this Agreement will be effective unless it is in writing and signed by County. No waiver of any breach, failure, right, or remedy will be deemed a waiver of any other breach, failure, right, or remedy, whether similar or not, nor will any waiver constitute a continuing waiver unless the writing signed by the County so specifies.

48. USE OF COUNTY'S NAME FOR COMMERCIAL PURPOSES

Contractor may not use the name of the County or reference any endorsement from the County in any fashion for

any purpose, without the prior express written consent of the County as provided by the County's authorized representative, or designee.

49. HEADINGS AND TITLES

The titles and headings in this Agreement are included principally for convenience and do not by themselves affect the construction or interpretation of any provision in this Agreement, nor affect any of the rights or obligations of the parties to this Agreement.

50. HANDWRITTEN OR TYPED WORDS

Handwritten or typed words have no greater weight than printed words in the interpretation or construction of this Agreement.

51. AMBIGUITIES

Any rule of construction to the effect that ambiguities are to be resolved against the drafting party does not apply in interpreting this Agreement.

52. ENTIRE AGREEMENT; MERGER

This Agreement and its Exhibits and Attachments (if any and including all contract release purchase orders) constitute the final, complete and exclusive statement of the terms of the agreement between the parties. It incorporates and supersedes all the agreements, covenants and understandings between the parties concerning the subject matter hereof, and all such agreements, covenants and understandings have been merged into this Agreement. No prior or contemporaneous agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

53. EXECUTION AND COUNTERPARTS

This Agreement may be executed in one or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. The parties agree that this Agreement, its amendments, and ancillary agreements to be entered into in connection with this Agreement will be considered signed when the signature of a party is delivered a method described herein.

Unless otherwise prohibited by law or County policy, the parties agree that an electronic copy of a signed contract, or an electronically signed contract, has the same force and legal effect as a contract executed with an original ink signature. The term "electronic copy of a signed contract" refers to a transmission by facsimile, electronic mail, or other electronic means of a copy of an original signed contract in a portable document format. The term "electronically signed contract" means a contract that is executed by applying an electronic signature using technology approved by the County.

54. NOTICES

All deliveries, notices, requests, demands or other communications provided for or required by this Agreement shall be in writing and shall be deemed to have been given when sent by registered or certified mail, return receipt requested; when sent by overnight carrier; or upon email confirmation to sender of receipt of a facsimile communication which is followed by a mailed hard copy from sender. Notices shall be addressed to the individuals identified in the Key Provisions of the Agreement as the County Contract Administrator and the Supplier Contact. Each party may designate a different person and address by sending written notice to the other party, to be effective no sooner than ten (10) days after the date of the notice.

55. ACCOUNT MANAGER

Contractor must assign an Account Manager to the County upon execution of the Agreement to facilitate the contractual relationship, be fully responsible and accountable for fulfilling the County's requirements. Contractor represents and warrants that such person will ensure that the County receives adequate pre-sales and post-sales support, problem resolution assistance and required information on a timely basis.

56. SURVIVAL

All representations, warranties, and covenants contained in this Agreement, or in any instrument, certificate, exhibit, or other writing intended by the parties to survive this Agreement, will survive the termination of this Agreement.

57. GOVERNING LAW, JURISDICTION AND VENUE

This Agreement shall be construed and interpreted according to the laws of the State of California, excluding its conflict of law principles. Proper venue for legal actions shall be exclusively vested in state court in the County of Sonoma. The parties agree that subject matter and personal jurisdiction are proper in state court in the County of Sonoma and waive all venue objections.

58. THIRD PARTY BENEFICIARIES

This Agreement does not, and is not intended to, confer any rights or remedies upon any person or entity other than the parties

59. AUTHORITY

Each party executing the Agreement on behalf of such entity represents that he or she is duly authorized to execute and deliver this Agreement on the entity's behalf, including, as applicable, the Board of Supervisors, the Board of Directors, or Executive Director. This Agreement shall not be effective or binding unless it is in writing and approved by the County's authorized representative, or authorized designee, as evidenced by their signature as set forth in this Agreement.

60. LIVING WAGE

Contractor agrees to comply with all applicable federal, state and local laws, regulations, statutes and policies, including but not limited to County of Sonoma Living Wage Ordinance, applicable to the services provided under this Agreement as they exist now and as they are changed, amended or modified during the term of this Agreement. Without limiting the generality of the foregoing, Consultant expressly acknowledges and agrees that this Agreement is subject to the provisions of Article XXVI of Chapter 2 of the Sonoma County Code, requiring payment of a living wage to covered employees. Noncompliance during the term of the Agreement will be considered material breach and may result in termination of the Agreement or pursuit of other legal or administrative remedies.

61. CONTRACTING PRINCIPLES

All entities that contract with the County to provide services where the contract value is $100,000 or more per budget unit per fiscal year and/or as otherwise directed by the Board, shall be fiscally responsible entities and shall treat their employees fairly. To ensure compliance with these contracting principles, all contractors shall: (1) comply with all applicable federal, state and local rules, regulations and laws: (2) maintain financial records, and make those records available upon request; (3) provide to the County copies of any financial audits that have been completed during the term of the Agreement; (4) upon the County's request, provide the County reasonable access, through representatives of the Contractor, to facilities, financial and employee records that are related to the purpose of the Agreement, except where prohibited by federal or state laws, regulations or rules.

62. CONTRACTOR TRAVEL EXPENSES

Contractor shall be solely responsible for any travel fees or out of pocket expenses.

63. INFORMATION SECURITY COMPLIANCE

(1) For purposes of this section, the following definitions shall apply:

a. "Breach" means unauthorized access to, or use of, County Data or information security networks or systems that compromises confidentiality, integrity, and/or availability those systems or County Data.
b. "Independent Penetration Testing," or "pen testing," means the County's practice - by using an independent third party - of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit
c. "Risk Assessment" means the process by which the County's Information Security Office ("ISO") assesses (i) the Contractor's information security program, and related aspects, by identifying,

analyzing, and understanding how the Contractor will store, process and transmit County Data; and (ii) the potential impact on the County of any security risks, weaknesses and threats related to safeguarding County assets and County Data. The Risk Assessment usually includes the ISO's evaluation of documentation provided by the Contractor.

(2) Contractor shall do all of the following:

a. Maintain or improve upon its information security posture at the time of the County's initial Risk Assessment as reasonably determined by the County. Contractor shall provide written notice to the County's Information Security Office ("ISO") of any changes or deficiencies to its information security posture.
b. Protect the confidentiality, integrity, availability of the County's data and comply with any information security requirements provided to Contractor by the ISO for the entire term of the Agreement.
c. Follow any updated security requirements for the remaining term of the Agreement if the County re-evaluates the Risk Assessment, conducts periodic audits, and/or completes annual Independent Penetration Testing.
d. Upon discovering any Breach that could impact the County, whether caused by Contractor, its officers, employees, contractors or agents or others, the Contractor shall notify the ISO at within 24 hours. Contractor shall also comply with all of its other obligations in this Agreement relating to breaches and potential breaches.

64. COUNTY DATA

(1) Sonoma County Sheriff's Office retains sole and exclusive ownership to all data provided during the term of this Agreement.

(2) Contractor shall not acquire any ownership interest in County Data (including County Confidential Information). As between Contractor and County, all County Confidential Information and/or County Data shall remain the property of the County. Contractor shall not, without County's written permission, use or disclose County Data (including County Confidential Information) other than in the performance of its obligations under this Agreement.

(3) Upon termination of this Agreement, Contractor shall promptly return all data to Sonoma County Sheriff's Office in a mutually agreeable format and media.

(4) Contractor shall be responsible for establishing and maintaining an information security program that is designed to ensure the security and confidentiality of County Data, protect against any anticipated threats or hazards to the security or integrity of County Data, and protect against unauthorized access to or use of County Data that could result in substantial harm or inconvenience to County or any end users. Upon termination or expiration of this Agreement, Contractor shall seek and follow County's direction regarding the proper disposition of County Data.

65. DATA AND SYSTEM SECURITY

(1) Contractor shall take appropriate action to address any incident of unauthorized access to County Data, including addressing and/or remedying the issue that resulted in such unauthorized access, and notifying County by phone or in writing within 24 hours of any incident of unauthorized access to County Data, or any other breach in Contractor's security that materially affects County or end users. If the initial notification is by phone, Contractor shall provide a written notice within 5 days of the incident. Contractor shall be responsible for ensuring compliance by its officers, employees, agents, and subcontractors with the confidentiality, privacy, and information security requirements of this Agreement. Should County Confidential Information and/or legally protected County Data be divulged to unauthorized third parties, Contractor shall comply with all applicable federal and state laws and regulations, including but not limited to California Civil Code sections 1798.29 and 1798.82 at Contractor's sole expense. Contractor shall not charge County for any expenses associated with Contractor's compliance with these obligations.

(2) Contractor shall defend, indemnify and hold County harmless against any claim, liability, loss, injury or damage arising out of, or in connection with, the unauthorized use, access, and/or disclosure of information by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or

damage caused by the sole negligence or willful misconduct of personnel employed by the County.

(3) The Contractor shall do all of the following:

- Implement and maintain an Audit Logging System within AWS GovCloud Environment that meets or exceeds the requirements outlined in the Criminal Justice Information Security (CJIS) Policy. AWS CloudTrail or equivalent audit logging service.

- Implement and maintain an Audit Logging System within ATIMS InCustody Service that meets or exceeds the requirements outlined in the Criminal Justice Information Security (CJIS) Policy. AWS CloudTrail or equivalent audit logging service.

- Maintain and monitor a Security Monitoring Service such as AWS SecurityHub or equivalent security monitoring service within AWS GovCloud Environment.

- Perform regular Vulnerability Scanning of the AWS GovCloud Environment using AWS Inspector or other vulnerability scanning service to ensure the detection and mitigation of security risks.

- Allow County of Sonoma to perform regular Vulnerability Scanning and Penetration Testing on all ATIMS provided GovCloud Environments with advanced notice to ATIMS by County.

- Perform regular Patch Management using AWS Systems Manager or other equivalent patch management service in compliance with the Criminal Justice Information Security (CJIS) Policy.

- Maintain Threat Detection Services such as AWS GuardDuty or equivalent services to identify and resolve suspicious and potentially malicious activity in the AWS GovCloud Environment.

(4) Contractor shall provide County with at least view-only access to any and all service health, security monitoring, threat detection and equivalent services utilized by Contractor in compliance with this Agreement.

66. BACKUP AND DISASTER RECOVERY

(1) Contractor shall backup and store all AWS Data in a different AWS GovCloud Region from the production databases at an interval agree upon in Section 6.4 Recovery Point Objective and Section 6.5 Recovery Time Objective of the Maintenance Agreement.

(2) Contractor shall regularly test backups to ensure data availability and integrity. The test should simulate data restoration procedures. In the event a backup test fails, the Contractor shall take immediate corrective action to resolve the issue and ensure the reliability of future backups.

(3) In the event of downtime, the contractor shall make reasonable efforts to restore services to an operational state within the time frame agreed upon in Section 6.4 Recovery Point Objective and Section 6.5 Recovery Time Objective of the Maintenance Agreement.

(4) Contractor shall work with County to develop and document a comprehensive Disaster Recovery Plan.

(5) Contractor shall offer the option of Service and Data Replication to a separate AWS GovCloud Region.

67. SYSTEM PERFORMANCE

(1) Contractor shall provide a system that is scalable to handle increased workloads and data storage requirements over the life of the agreement. Contractor shall monitor performance metrics and adjust system capacity, at no cost to the County, as to maintain user experience so that any system delays do not hinder the workflow of the users.

(2) Contractor understands that County operates in a 24x7x365 high-volume environment and will adhere to Response and Resolution Times in Section 6.1 of the Maintenance Agreement.

68. SERVICE LEVEL AGREEMENT

(1) Contractor shall ensure the system maintains 99.9% availability on a 24x7x365 basis as stated in Section 6.3 Hosting – Service Guarantee of the Maintenance Contact.

(2) Contractor shall provide support in adherence to Section 6.1 Support – ATIMS Tier 2 Response and Resolution Times of the Maintenance Contract.

69. CJIS DATA AND COMPLIANCE

(1) The Agreement is contingent upon both County and Contractor's approval of the California Department of Justice (CalDOJ) CLETS data application.

(2) Contractor is to keep up to date on all Criminal Justice Information Security (CJIS) required training and is subject to all CJIS background requirements.

(3) Contractor will cooperate and comply with any and all audit requests made by CalDOJ or FBI and immediately rectify any issues found to be not in compliance at no additional cost to County. Contractor to immediately notify county of any such requests.

70. COUNTY POLICIES

(1) Contractor shall adhere to County Policy 9-2 Information Technology Use and Security Policy.

(2) Contractor shall adhere to County Policy 9-4 Information Technology Professional Policy.

(3) Contractor shall adhere to County Policy 9-6 Information Technology Artificial Intelligence (AI) Policy.

71. ACCESS TO COMPETITIVELY BID AGREEMENTS

Where the contract award is a result of a formal competitive solicitation, Contractor may opt to permit the use of this Agreement by other political subdivisions, municipalities, tax supported agencies and non-profit entities in the United States. Such participating agencies shall make purchases in their own name, make payments directly to the Contractor and shall be liable directly to Contractor holding the County of Sonoma harmless.

If applicable, Contractor shall be required to maintain a list of cooperative entities using this Agreement. The list shall report dollar volumes spent annually and shall be provided on an annual basis to the County, at the County's request.

72. COMPLIANCE WITH ALL LAWS AND REGULATIONS INCLUDING NONDISCRIMINATION, EQUAL OPPORTUNITY, AND WAGE THEFT PREVENTION

Contractor's violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the Agreement. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 *et seq*. the Fair Packaging and Labeling Act. and the standards and regulations issued there under. Contractor agrees to defend, indemnify and hold harmless the County for any loss, damage, fine, penalty, or any expense whatsoever as a result of Contractor's failure to comply with the act and any standards or regulations issued there under.

(1) Compliance with All Laws: Contractor shall comply with all applicable Federal, State, and local laws, regulations, rules, and policies (collectively, "Laws"), including but not limited to the non- discrimination, equal opportunity, and wage and hour Laws referenced in the paragraphs below.

(2) Compliance with Non-Discrimination and Equal Opportunity Laws: Contractor shall comply with all applicable Laws concerning nondiscrimination and equal opportunity in employment and contracting, including but not limited to the following: Sonoma County's policies for contractors on nondiscrimination and equal opportunity; Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; the Age Discrimination in Employment Act of 1967; the Rehabilitation Act of 1973 (Sections 503 and

504); the Equal Pay Act of 1963; California Fair Employment and Housing Act (Government Code sections 12900 et seq.); California Labor Code sections 1101, 1102, and 1197.5; and the Genetic Information Nondiscrimination Act of 2008. In addition to the foregoing, Contractor shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political belief, organizational affiliation, or marital status in the recruitment, selection for training (including but not limited to apprenticeship), hiring, employment, assignment, promotion, layoff, rates of pay or other forms of compensation. Nor shall Contractor discriminate in the provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.

(3) Compliance with Wage and Hour Laws: Contractor shall comply with all applicable wage and hour Laws, which may include but are not limited to, the Federal Fair Labor Standards Act, the California Labor Code, and, if applicable, any local Minimum Wage, Prevailing Wage, or Living Wage laws.

(4) Definitions: For purposes of this Section, the following definitions shall apply. A "Final Judgment, Decision, Determination, or Order" shall mean a judgment, decision, determination, or order (a) which is issued by a court of law, an investigatory government agency authorized by law to enforce an applicable Law, an arbiter, or arbitration panel and (b) for which all appeals have been exhausted or the time period to appeal has expired. For pay equity Laws, relevant investigatory government agencies include the federal Equal Employment Opportunity Commission, the California Division of Labor Standards Enforcement, and the California Department of Fair Employment and Housing. Violation of a pay equity Law shall mean unlawful discrimination in compensation on the basis of an individual's sex, gender, gender identity, gender expression, sexual orientation, race, color, ethnicity, or national origin under Title VII of the Civil Rights Act of 1964 as amended, the Equal Pay Act of 1963, California Fair Employment and Housing Act, or California Labor Code section 1197.5, as applicable. For wage and hour Laws, relevant investigatory government agencies include the federal Department of Labor, the California Division of Labor Standards Enforcement and the City of San Jose's Office of Equality Assurance.

(5) Prior Judgments, Decisions or Orders against Contractor: By signing this Agreement, Contractor affirms that it has disclosed any final judgments, decisions, determinations, or orders that (a) were issued in the five years prior to executing this Agreement by a court or investigatory government agency and (b) found that Contractor violated an applicable wage and hour or pay equity law. Contractor further affirms that it has satisfied and complied with – or has reached agreement with the County regarding the manner in which it will satisfy – any such final judgments, decisions, determinations, or orders.

(6) Violations of Wage and Hour Laws or Pay Equity Laws During Term of Agreement: If at any time during the term of this Agreement, Contractor receives a Final Judgment, Decision, Determination, or Order rendered against it for violation of an applicable wage and hour Law or pay equity Law, then Contractor shall promptly satisfy and comply with any such Final Judgment, Decision, Determination or Order. Contractor shall inform the Office of the County Executive- Office of Countywide Contracting Management (OCCM) of any relevant Final Judgment, Decision, Determination, or Order against it within 30 days of the Final Judgment, Decision, Determination, or Order becoming final or of learning of the Final Judgment, Decision, Determination, or Order, whichever is later. Contractor shall also provide any documentary evidence of compliance with the Final Judgment, Decision, Determination, or Order within 5 days of satisfying the Final Judgment, Decision, Determination, or Order. Any notice required by this paragraph shall be addressed to. Notice provisions in this paragraph are separate from any other notice provisions in this Agreement and, accordingly, only notice provided to the Office of the County Executive-OCCM satisfies the notice requirements in this paragraph.

(7) Access to Records Concerning Compliance with Pay Equity Laws: In addition to and notwithstanding any other provision of this Agreement concerning access to Contractor's records, Contractor shall permit the County and/or its authorized representatives to audit and review records related to compliance with applicable pay equity Laws. Upon the County's request, Contractor shall provide the County with access to any and all facilities and records, including but not limited to financial and employee records, that are related to the purpose of this Section, except where prohibited by federal or state laws, regulations or rules. County's access to such records and facilities shall be permitted at any time during Contractor's normal business hours upon no less than 10 business days' advance notice.

(8) Pay Equity Notification: Contractor shall (1) directly provide each employee working in California and each person applying for a job in California with a written copy of any applicable pay equity Laws, or (2)

electronically disseminate the text of applicable pay equity Laws to each California employee and job applicant, either directly or by posting a copy in conspicuous places available to employees and applicants. Such notification shall occur at least once during the term of this Agreement and, if this Agreement is a multi-year Agreement, at least annually thereafter.

(9) Material Breach Failure to comply with any part of this Section shall constitute a material breach of this Agreement. In the event of such a breach, the County may, in its discretion, exercise any or all remedies available under this Agreement and/or at law. County may, among other things, take any or all of the following actions:

(i) Suspend or terminate any or all parts of this Agreement.

(ii) Withhold payment to Contractor until full satisfaction of a Final Judgment, Decision, Determination, or Order

(iii) Offer Contractor an opportunity to cure the breach.

(10) Subcontractors: Contractor shall impose all of the requirements set forth in this Section on any subcontractors permitted to perform work under this Agreement. This includes ensuring that any subcontractor receiving a Final Judgment, Decision, Determination, or Order for violation of an applicable wage and hour Law promptly satisfies and complies with such Final Judgment, Decision, Determination, or Order.

73. LICENSE GRANT

Contractor grants to County a perpetual, non-exclusive, royalty-free, fully paid-up license to use the Software for its business activities, which includes fulfilling its mission of providing services to the public. This includes the right to use licensed software in backup, disaster recovery, and testing environments.

74. CLICK-THROUGH AGREEMENTS AND CONTRACTOR POLICIES

(1) No provisions of any shrink-wrap or any click-through agreement (or other form of "click to accept" agreement) that may routinely accompany any products or services acquired under this Agreement shall apply in place of, or serve to modify any provision of this Agreement, even if a user or authorized officer of County purports to have affirmatively accepted such shrink-wrap or click through provisions. Without limiting the foregoing, no "terms of use," "privacy policy" or other policy on Contractor's website or application (collectively, "Policies") or another website that may routinely accompany any products or services acquired under this Agreement shall apply in place of or serve to modify any provision of this Agreement.

(2) For the avoidance of doubt and without limiting the foregoing, in the event of a conflict between any such shrink-wrap, click-through provisions or Policies (irrespective of the products or services that such provisions attach to) and any term or condition of this Agreement, the relevant term or condition of this Agreement shall govern to the extent of any such conflict. Only the provisions of this Agreement as amended from time to time, and executed by the parties, shall apply to County and or authorized user.

(3) The parties acknowledge that the County and or authorized users may be required to click "Accept" as a routine condition of access to services through the Contractor's website or other application. Such click-through provisions or Policies on Contractor's website shall be null and void for County and/or each such authorized user and shall only serve as a mechanical means for accessing such services.

75. BUSINESS ASSOCIATE AGREEMENT

Contractor shall comply with the Business Associate Agreement attached as Exhibit G to the Agreement.

76. ACCESSIBILITY

Contractor is responsible for satisfying all federal and California accessibility laws set forth under section 508 of the Rehabilitation Act of 1973, and California Government Code section 7405. All materials and technology produced or provided by Contractor under the Agreement must be created and delivered in a manner that meets the accessibility requirements set forth under these laws. These requirements include but are not limited to closed captioning of all presentations, training materials, curriculum, and all other materials and technology as defined under the law. All websites developed and maintained by Contractor must be accessible, built to the most current and highest Web Content Accessibility Guidelines (WCAG), and delivered with documentation

allowing the County to certify them as accessible and in compliance with California Government Code sections 7405 and 11135. Contractor is responsible for all claims and expenses borne by the County arising out of the work performed under the Agreement that is found not to be in compliance with federal and California law. These costs include but are not limited to legal costs, court costs, and costs for remediation of the work produced.

Exhibit B
Payment and Fee Schedule

Exhibit B sets forth the fee structure and payment terms for the Implementation and Support Services (including Hosting and Maintenance) of the ATIMS Jail Management System (JMS).

ATIMS CONFIDENTIAL Cost Proposal Summary

Sonoma County, California - *ATIMS InCustody Plus+*

Unlimited Users

Number of Active Inmates: up to 900

Updated 04/15/25

1. Jail Management Software Costs	One time Price	Required	Sub-Total Price	Discounted Special On Prem Pricing	Annual recurring fee
Jail Management Software	$ 517,500	YES	$ 517,500		$ 194,063
Category 1 Sub-Total			$ 517,500	$ -	$ 194,063
2. Add-On Functionalizes Licenses	**Price**	**Required**	**Sub-Total Price**	**Discounted Special Pricing**	**Annual recurring fee**
A1 - ATIMS Biometrics					
Fingerprint identification and Registration at Intake, Release, and Kiosks. Personnel Fingerprint recognition when logging into JMS. *	$ 5,000	NO	0	0	0
A2 - Biometrics Software License (Fulcrum)					
This is a one time software license fee to Fulcrum for biometrics functionality. (This is software only. Hardware costs are provided in Category 8).	$ 7,250	NO	0	0	0
A3 - Biometrics Readers - per reader software license (Fulcrum)					
This is an annual hardware cost ($110) - (in hardware below) + license fee ($125) paid to Fulcrum for biometrics reader functionality. Licenses required are 1:1 with the quantity of biometric readers. Following the first year's fees, ATIMS pays this annual fee on the client's behalf as part of the Annual Support & Maintenance Agreement, if kept current by the client.	$ 1,250	NO	0	0	0
B -Public Inmate Visit Scheduling (Saas Only No one time cost)					
Provide external website for Public to schedule visits	$ 27,000	YES	$ 27,000	0	$ 27,000
C - ATIMS Mobile Web					
Provide functionality on any Handheld devise used by correctional staff for POD related tasks such as: tracking roster, inmate file, headcounts, cell logs, safety checks, and many more. **	$ 25,000	YES	$ 25,000	0	$ 8,750
D - ATIMS License for Dynamic Imaging Camera Option					
The Mugshot Photo is taken using DISI software and controlled camera, is embedded into ATIMS software. The mugshot is attached to JMS and integrates with inmate intake and booking functionality.* Hardware & 3rd party vendor costs below	$ 15,000	NO	0	0	0
E-ATIMS Inmate Lookup External Website (Saas Only No one time cost)					
Includes a tool kit that develops an external, configurable website that allows the public to search for specified data about the current inmate population. The look and feel can be configured to your agency. This site is fed from the JMS; but there is no direct link into the JMS; the data is separated and fed to the website. If the data exists in ATIMS JMS; it can be included in the export. Example website: https://wic.sjgov.org	$ 21,600	YES	$ 21,600	0	$ 21,600
F-Inmate Self Service Kiosk/Tablet (POD) Software (Saas Only No one time cost)					
ATIMS base kiosk/tablet application includes secure Booking, Visitation, Appointments, Incident, and Grievance information. In addition it allows the inmates to place requests and receive responses. *This can also be added to a commissary or phone vendors POD Kiosk or tablet. **Kiosk hardware is typically procured through the Commissary or Trust Accounting Vendor.	$ 21,600	YES	$ 21,600	0	$ 21,600
G- Local Data Base Replication (Saas Only No one time cost)					
Replicaiton of the production database locally at the agency	$ 50,000	YES	$ 50,000	0	$ 50,000
Category 2 Sub-Total				$ -	$ 178,950
3. Customizations	**Price**	**Required**	**Sub-Total Price**	**Total Pricing**	
Reporting - 10 custom included at no additional cost; for ea 5 reports-additional $10k. We have 250+ standard reports and train your staff to build reports.	$ 20,000	YES	$ 20,000	$ 20,000	
Forms - 10 custom included at no additional cost; for ea 5 forms-additional $10k. Assumes medium complexity.	$ 20,000	YES	$ 20,000	$ 20,000	
Category 3 Sub-Total			$ 20,000	$ 40,000	

4. Interfaces		Price	Required	Sub-Total Price	Total Pricing	
RMS - Central Square (on prem)		$ 20,000	YES	$ 20,000	$ 20,000	
Inmate Phone (ViaPath) - 2 way		$ 10,000	YES	$ 10,000	$ 10,000	
Video Visitation (ViaPath) - 1 way		$ 5,000	YES	$ 5,000	$ 5,000	
Inmate Self Service (ViaPath) - 2-way	Not required if 2. F selected	$ 15,000	NO	0	0	
Commissary & Kitchen (Summit) - 2 way		$ 10,000	YES	$ 10,000	$ 10,000	
Inmate Trust Accounting / Kiosk (Lockdown) - 2 way		$ 10,000	YES	$ 10,000	$ 10,000	
Courts (Odyssey) - 2 way		$ 10,000	YES	$ 10,000	$ 10,000	
Probation		$ 10,000	YES	$ 10,000	$ 10,000	
Livescan - 2 way		$ 10,000	YES	$ 10,000	$ 10,000	
Local Warrants		$ 20,000	YES	$ 20,000	$ 20,000	
VINE - 1 way		$ 5,000	YES	$ 5,000	$ 5,000	
Rounds Tracker	Not Required if 2. C selected	$ -	NO	0	0	
CLETS/Wants & Warrants		$ 40,000	YES	$ 40,000	$ 40,000	
Category 4 Sub-Total				$ 150,000	$ 150,000	

Category 5 - Professional Services	# of Personnel	Hours of Effort	Price	Required	Sub-Total Price	Total Discounted Pricing	
1. Project Management	1	1500	$ 375,000	YES	$ 375,000	$ 281,250	
2. Business Analysis	2	600	$ 210,000	YES	$ 210,000	$ 157,500	
3. Technical Lead	1	1640	$ 328,000	YES	$ 328,000	$ 246,000	
4. Technical Support	2	500	$ 165,000	YES	$ 165,000	$ 123,750	
5. Training	3	200	$ 60,000	YES	$ 60,000	$ 45,000	
6. Data Conversion	1	600	$ 120,000	YES	$ 120,000	$ 90,000	
7. Documentation	1	250	$ 18,750	YES	$ 18,750	$ 14,063	
Category 5 Sub-Total					$ 957,563	$ 957,563	

Category 6 - Travel	# of Personnel	# of Days	Price	Required	Sub-Total Price	Total Discounted Pricing	
Kick Off Meeting	4	3	$ 9,021	YES	$ 9,021	$ 6,766	
Business Analysis	2	35	$ 46,223	YES	$ 46,223	$ 34,667	
Go Live	4	10	$ 27,270	YES	$ 27,270	$ 20,453	
Project Management	1	35	$ 23,111	YES	$ 23,111	$ 17,333	
Technical On Site	2	30	$ 39,705	YES	$ 39,705	$ 29,779	
Training On Site	4	10	$ 27,270	YES	$ 27,270	$ 20,453	
Category 6 Sub-Total					$ 172,600	$ 129,450	

Notes: * Software costs only. Hardware costs are broken out and provided in Category 7 pricing
** Hardware, network, and other infrastructure components are not included in price - unless SaaS hosting is selected. Offline functions to be scoped and priced.

TOTAL ESTIMATED ANNUAL SAAS HOSTED PRICE		$ 373,013
One time costs for SaaS implementation W/O hardware		$ 1,277,012

(SAAS HOSTED ANNUAL COST PAYMENT SCHEDULE		
Year 1	$	373,012.50
Year 2	$	380,472.75
Year 3	$	388,082.21
Year 4	$	395,843.85
Year 5	$	403,760.73

5 yr Est Cost	$	1,941,172

7. Hardware Costs (included for budget purposes)	Price	Quantity	Sub-Total Price	Pricing	
Officer Mobile Tablet(s) - requires wifi	$ 2,300	$ 20	$ 46,000	$ 46,000	
5 year Mainenance for Officer Mobile	$ 700	$ 20	$ 14,000	$ 14,000	
Extra Battery	$ 130	$ 20	$ 2,600	$ 2,600	
Device and Extra Battery Charging Cradle	$ 233	$ 20	$ 4,660	$ 4,660	
Wristbands (1 box / 500)	$ 250	$ 10	$ 2,500	$ 2,500	
Label Printer	$ 700	$ 3	$ 2,100	$ 2,100	
Barcode [RFID] Scanner/Reader	$ 300	$ -	$ -	$	-
Wristband Sealer	$ 350	$ 3	$ 1,050	$ 1,050	
Topaz Signature Pads	$ 250	$ 20	$ 5,000	$ 5,000	
Category 7 Sub-Total			$ 71,860	$ 71,860	

Includes software use (up to 900), add on functional license use, 3rd party vendor license use, and maintenance & support costs, hosted server costs

TOTAL INCL 1 TIME COST	$	3,290,044

General Fee Schedule Terms:

- This is a Fixed Fee Project.
- The total contract value (assuming renewal of the optional terms) is $3,290,044 ($1,277,012 in Implementation fees and $1,941,172 in total Annual Recurring fees)
- The Fixed Fee is based on the ATIMS pricing proposal, the roles and responsibilities of ATIMS and the County, as stated in the Statement of Work (SOW), and representations, communications, and pricing provided by ATIMS during the procurement process.
- Annual Recurring fees including SaaS Hosting are not accrued or incurred by County until completion of the

project and post go-live.

- Invoices are to be submitted only upon County's formal acceptance, in writing, of a Deliverable or Milestone.
- Formal Acceptance of all work, including interfaces, configurations, forms, reports, and enhancements, is subject to the County's Acceptance Criteria and process as set forth in the SOW and/or Deliverable Expectation Document (DED).
- Payments are processed in accordance with the terms of the Agreement.
- ATIMS assumes responsibility of any taxes other than applicable Sales Tax, which is a County responsibility

Implementation Fees

Fee Type	Amount	Notes
1. Project Management	$375,000	Includes a full-time dedicated Project Manager and related project management services for the duration of the implementation and stability period.
2. Implementation	$692,012	Includes: 1) With the exception of Project Management and Training, all Implementation and related services, including, but not limited to, Software installation & administration, Business Analysis, Technical Lead/Support; Data Conversion; Testing / Quality Control, Go Live Support, Post Go Live deliverables, Stability Period Support. 2) All separately priced RFP Forms ($40,000)
3.Interfaces	$150,000	Includes all RFP specified Interfaces and related data exchanges (an interface to a source system may have one or more data exchanges).
4. Training	$60,000	Includes all required training, documentation and materials.
Total	**$1,277,012**	

Notes:

- Implementation Fees are subject to a 15% retainage which will be withheld from each payment and is due on Final Acceptance. See Implementation Payment Schedule.
- At the point of Testing, the Test environment will mirror Production specifications. The Production server will be brought online at least 60 days before the scheduled Go Live.
- All Interfaces, configurations, and forms must be explicitly authorized by the County during the implementation.
- If the County removes, or otherwise withholds authorization, of an interface, configuration, or form ("Adjusted Items"), the overall fixed fee will not change, unless otherwise explicitly agreed to in a Change Order or by the Parties, and the quoted hours/fees for any such Adjusted Item will be reallocated to other implementation services (e.g., additional configurations, including reports and forms) or enhancements, that may be performed during implementation or post Go Live.

Implementation Payment Schedule

Milestones by Phase & Track	Payment %	$ (Less Retainage)	Payment % per Phase	Amount per Phase
PHASE 1			7.5%	$81,409.52
1) Planning	5.0%	$54,273.01		
2) Installation	2.5%	$27136.51		
PHASE 2			15.0%	$162,819.03
3A) Business Analysis	7.5%	$81,409.50		
3B) Modifications	2.5%	$27,136.51		
3C) Interfaces	2.5%	$27163.51		
3D) Migration	2.5%	$27136.51		
PHASE 3			45.0%	$488,457.09
4)Configuration	10.0%	$108,546.02		
5A) Modifications	5.0%	$54,273.01		
5B) Interfaces	7.5%	$81,409.52		
5C) Migration	7.5%	$81,409.52		
5D) Forms & Reports	5.0%	$54,273.00		
6) Test	10.0%	$108,564.02		
PHASE 4			32.5%	$352,744.57
7) Train	5.0%	$54,273.01		
8) Go Live	15.0%	$162,819.03		
9) Post Go Live	0.0%			
10) Project Close	12.5%	$135,682.53		
Total Milestone Payments	**100.0%**	**$1,085,460.20**		
Retainage - Paid on Final Acceptance - After 90 Day Stability Period	15%	$191,551.80		
Total Implementation Payments		**$1,277,0122**		

Notes:

- Payment is only to be made on Formal Acceptance of a Milestone (See General Fee Schedule Terms).
- Actual Milestone payment amounts may be adjusted to reflect any relevant Change Orders, as described in the Statement of Work.

Annual Recurring Fees

Annual Recurring Fees are $373,013 per year, and include the following services (See Support Agreement for details):

Fee Type	Notes
1.SaaS Subscription Fee	Includes use of JMS Software, authorized add-on licenses, JMS Enhancements
2. Hosting Services	Includes server, database, network, storage, security, auditing, load balancing and related services.
3. Support & Maintenance	Includes Updates and Fixes (See Support Agreement)
4. Professional Services	Includes County specified development (interfaces, enhancements, configurations, forms, reports), training, and documentation (110 hours @ $200/hour).

Notes:

- The Support Agreement details the ongoing services to be provided by ATIMS to the County.
- Add-On Licenses must be authorized by the County.
- The SaaS Subscription Fee includes unlimited County users and a 900 JMS active inmate population cap.
- An increase in SaaS fees of $215.63 per inmate will only occur with a sustained Average Daily Population (ADP) increase over one (1) month at a pro-rated charge for the month.
- Reductions in Recurring Annual Fees may be negotiated by ATIMS and the County and memorialized via a Change Order or Contract Amendment.
- Prior to the conclusion of the Agreement term, including any optional periods, the parties shall agree upon an updated fee schedule for Annual Recurring Fees.

Notes – Start of Annual Recurring Fees

- Go Live is the authorized use of the JMS by the County in a live Production Environment.
- Annual Recurring Fees will commence on the Go Live date
- Annual Recurring Fees will be prorated over the Support term from the Go Live date to the contract end date (including optional renewal periods), based on the occurrence of the Go Live date per the following schedule.

Go Live Date from Kickoff	Total Term Recurring Fees	Notes
4 Years	$395,843.85	Monthly $32,986.99
4 Years, 1 month	$362,856.86	Reduction of 1 month prorated fees

4 Years, 2 months	$329,869.87	Reduction of 2 months prorated fees
4 Years, 3 months	$296,882.88	Reduction of 3 months prorated fees
4 Years, 4 or more months	$296,882.88	No further reduction

Enhancement Fees:

As noted in the description of Annual Recurring Fees (p.4), "1. SaaS Subscription Fees" includes Enhancements.

Notes:

- Enhancement Fees reflect work to "customize" (modify) the base JMS product to meet a County requirement.
- The actual scheduling and Notice to Proceed for Enhancement work to be performed by ATIMS must be approved by the County in writing.
- The County will only be charged for Enhancements authorized and accepted by the County.
- $250,000 of the total Enhancement Fees is included in the Implementation Fees (See: "Implementation"), the remainder is included in the Recurring SaaS Subscription Fees.
- During the implementation, the County may adjust the work subject to an Enhancement Fee, by removing, adding, or modifying a requirement. Reductions in Enhancement Fees through removal or modification of a related requirement will be applied to the Implementation Fees first.

  At sixty (60) days before Go Live, or as agreed by ATIMS and the County, should the County, due to removal or modification of Enhancement requirements, be due a credit beyond the $250,000 value of the Implementation Enhancements, the annual recurring fees will be adjusted by means of a Change Order to reflect the actual authorized Enhancements and Add-On Licenses. Example: An increase of $100,000 in new Enhancements and a removal of $400,000 in currently identified Enhancements will lead to a reduction of $250,000 in Enhancement value from the Implementation Fees, and a backing out of $50,000 in recurring annual fees over the support period, including any multipliers and add-on fees/charges or percentages, similar to the ATIMS provided pricing calculations.

Professional Service Fees

Implementation Period

There may be instances during the implementation period where the County requests professional services that are outside the scope of the Statement of Work. If the parties determine that such Professional Services are outside the scope of the Statement of Work, and such services are authorized by the County, for example via a Change Order, during the implementation period, such services will be provided at the following ATIMS proposed discounted pricing rate:

- Configurations (including Interfaces and Reports): $160/hour
- Enhancements: $100/hour
- Forms: $125/hour.

Support Period

There may be instances during the support period where the County requests professional services that are included as a Service Credit against the paid annual fees (See Support Agreement, section 5.8 Service Credits) or are outside the scope of the Support Agreement. As set forth in the Support Agreement, the County may authorize such professional services (e.g., development work, configurations, forms, training), to be provided by ATIMS at a blended rate of $165 per hour.

Exhibit C
Insurance Requirements

With respect to performance of work under this Agreement, Consultant shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a *Waiver of Insurance Requirements*. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

County reserves the right to review any and all of the required insurance policies and/or endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve Consultant from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

Workers Compensation and Employers Liability Insurance

Required if Consultant has employees as defined by the Labor Code of the State of California.

Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.

Employers Liability with minimum limits of $1,000,000 per Accident; $1,000,000 Disease per employee; $1,000,000 Disease per policy.

Required Evidence of Insurance: Certificate of Insurance.

If Consultant currently has no employees as defined by the Labor Code of the State of California, Consultant agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

General Liability Insurance

Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) form CG 00 01.

Minimum Limits: $1,000,000 per Occurrence; $2,000,000 General Aggregate; $2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance. If Consultant maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by Consultant.

Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds $100,000 it must be approved in advance by County. Consultant is responsible for any deductible or self-insured retention and shall fund it upon County's written request, regardless of whether Consultant has a claim against the insurance or is named as a party in any action involving the County.

The County of Sonoma, it's Officers, Agents and Employees, Attn: Sonoma County Sheriff's Office, 2796 Ventura Avenue Santa Rosa, CA 95403 shall be endorsed as additional insureds for liability arising out of operations by or on behalf of the Consultant in the performance of this Agreement.

The insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.

The policy definition of "insured contract" shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage including the "f" definition of insured contract in ISO form CG 00 01, or equivalent).

The policy shall cover inter-insured suits between the additional insureds and Consultant and include a "separation of insureds" or "severability" clause which treats each insured separately.

Required Evidence of Insurance:

Certificate of Insurance.

Automobile Liability Insurance

Minimum Limit: $1,000,000 combined single limit per accident. The required limits may be provided by a combination of Automobile Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.

Insurance shall cover all owned autos. If Consultant currently owns no autos, Consultant agrees to obtain such insurance should any autos be acquired during the term of this Agreement or any extensions of the term.

Insurance shall cover hired and non-owned autos.

Required Evidence of Insurance: Certificate of Insurance.

Professional Liability/Errors and Omissions Insurance

Minimum Limit: $1,000,000 per claim or per occurrence.

Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured

retention exceeds $100,000 it must be approved in advance by County.

If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

Cyber Liability Insurance

Network Security & Privacy Liability Insurance:

Minimum Limit: $2,000,000 per claim per occurrence, $2,000,000.00 aggregate.

Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Consultant in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.

If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

Technology Errors and Omissions Insurance:

Minimum Limit: $2,000,000 per claim or per occurrence, $2,000,000.00 aggregate.

Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Consultant in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.

The Policy shall include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the County in the care, custody, or control of the Consultant. If the Consultant maintains broader coverage and/or higher limits than the minimums shown above, the Entity requires and shall be entitled to the broader coverage and/or the higher limits maintained by the contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the Entity

If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

Standards for Insurance Companies

Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

Documentation

The Certificate of Insurance must include the following reference: Jail Management System.

All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Consultant agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.

The name and address for Additional Insured endorsements and Certificates of Insurance is: **The County of Sonoma, It's Officers, Agents and Employees; Attn: Sonoma County Sheriff's Office, 2796 Ventura Avenue, Santa Rosa, CA 95403.**

Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists, at least ten (10) days before expiration or other termination of the existing policy.

Consultant shall provide immediate written notice if: (1) any of the required insurance policies is terminated; (2) the limits of any of the required policies are reduced; or (3) the deductible or self-insured retention is increased.
Upon written request, certified copies of required insurance policies must be provided within thirty (30) days.

Policy Obligations

Consultant's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

Material Breach

If Consultant fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. County, at its sole option, may terminate this Agreement and obtain damages from Consultant resulting from said breach. Alternatively, County may purchase the required insurance, and without further notice to Consultant, County may deduct from sums due to Consultant any premium costs advanced by County for such insurance. These remedies shall be in addition to any other remedies available to County.

Exhibit D
FBI CJIS Security Addendum

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI 1000

Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

Exhibit E

STATE OF CALIFORNIA
HDC 0004B
(Orig. 11/2005; Rev. 03/2010)

CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

Print Form

Agreement to allow California Law Enforcement Telecommunications System (CLETS) access by

Sonoma County Sheriff's Office (Public law enforcement/criminal justice agency) , CA0490000 (ORI)

to ATIMS (Private Contractor)

to perform Jail Management system implementation and operation (Type of service) services on its behalf.

Access to the CLETS is authorized to public law enforcement and criminal justice agencies (*hereinafter referred to as the CLETS subscribing agency*) only, which may delegate the responsibility of performing the administration of criminal justice functions (e.g., dispatching functions or data processing/information services) in accordance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Addendum to a private contractor. The private contractor may access systems or networks that access the CLETS on behalf of the CLETS subscribing agency to accomplish the above-specified service(s). This agreement must be received by the California Department of Justice (CA DOJ) prior to the subscribing agency permitting access to the CLETS. The performance of such delegated services does not convert that agency into a public criminal justice agency, not automatically authorize access to state summary criminal history information. Information from the CLETS is confidential and may be used only for the purpose(s) for which it is authorized. Violation of confidentiality requirements or access authorizations may be subject to disciplinary action or criminal charges.

Pursuant to the policies outlined in the *CLETS Policies, Practices, and Procedures (PPP)* and the Federal Bureau of Investigation's (FBI) *CJIS Security Policy*, it is agreed the CLETS subscribing agency will maintain responsibility for security control as it relates to the CLETS access. Security control is defined as the ability of the CLETS subscribing agency to set, maintain, and enforce:

1. Standards for the selection, supervision, and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant CLETS access to personnel who meet these standards and deny it to those who do not.

2. Policies governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support a telecommunications network and related CA DOJ criminal justice databases used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Security control includes, but is not limited to, the supervision of applicable equipment, systems design, programming, and operating procedures associated with the development, implementation, and operation of any computerized message-switching or database systems utilized by the served law enforcement agency or agencies. Computer sites must have adequate physical security to protect against any unauthorized viewing or access to computer terminal, access devices, or stored/printed data.

CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

Additionally, it is the responsibility of the CLETS subscribing agency to ensure that all private contractors receiving information from the CLETS meet the minimum training, certification, and background requirements that are also imposed on the CLETS subscribing agency's staff. The minimum requirements are applicable also to staff having access to record storage areas containing information from the CLETS. The minimum requirements include, but are not limited to:

1. Prior to allowing the CLETS access, train, functionally test, and affirm the proficiency of all the CLETS computer operators to ensure compliance with the CLETS and the FBI's National Crime Information Center (NCIC) policies and regulations, if applicable. Biennially, provide testing and reaffirm the proficiency of all the CLETS operators, if applicable.

2. State and FBI criminal offender record information searches must be conducted prior to allowing access to the CLETS computers, equipment, or information. If the results of the criminal offender record information search reveal a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted.

3. Each individual must sign a CLETS Employee/Volunteer Statement form (HDC 0009) prior to operating or having access to CLETS computers, equipment, or information.

In accordance with CLETS/NCIC policies, the CLETS subscribing agency has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the private contractor. The private contractor agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement and to accomplish the directives for service under the provisions of this agreement. The CLETS Management Control Agreement (HDC 0004B) shall be updated when the head of either agency changes or immediately upon request from the CA DOJ.

By signing this agreement, the vendors and private contractors certify they have read and are familiar with the contents of (1) the FBI's CJIS Security Addendum, (2) the NCIC 2000 Operating Manual, (3) the FBI's CJIS Security Policy, (4) Title 28, Code of Federal Regulations, Part 20, and (5) the CLETS PPP and agree to be bound by their provisions. Criminal offender record information and related data, by its very nature, is sensitive and has potential for great harm if misused. Access to criminal offender record information and related data is therefore limited to the purpose(s) for which the CLETS subscribing agency has entered into the contract. Misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; use, dissemination, or secondary dissemination of information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. Accessing the system for an appropriate purpose and then using, disseminating, or secondary dissemination of information received for another purpose other than execution of the contract also constitutes misuse. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Signature (CLETS Subscribing Agency Head)	Signature (Private Contractor Agency Head)
Print Name and Title	Felix Rabinovich Print Name and Title
Date	Jan 3, 2025 Date

Exhibit F

STATE OF CALIFORNIA
Exhibit I – HDC 0009
(Rev. 02/2019)

DEPARTMENT OF JUSTICE

CLETS EMPLOYEE/VOLUNTEER STATEMENT

Print Form

Use of information from the California Law Enforcement Telecommunications System (CLETS) and the Department of Motor Vehicles record information

As an employee/volunteer of Sonoma County Sheriff's Office , you may have access to confidential criminal records, the Department of Motor Vehicle (DMV) records or other criminal justice information, much of which is controlled by statute. All information from the CLETS is based on the "need-to-know" and the "right-to-know" basis. Federal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644. The misuse of such information may adversely affect an individual's civil rights and violates the law and/or CLETS policies.

Penal Code (PC) section 502 prescribes the penalties relating to computer crimes. PC sections 11105 and 13300 identify who has access to state and local summary criminal history information and under which circumstances it may be released. PC sections 11141–11143 and 13302–13304 prescribe penalties for misuse of state and local summary criminal history information. Government Code section 6200 prescribes the felony penalties for misuse of public records and information from the CLETS. California Vehicle Code section 1808.45 prescribes the penalties relating to misuse of the DMV record information.

PC sections 11142 and 13303 state:

> **"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."**

Any employee/volunteer who is responsible for the CLETS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL INFORMATION FROM THE CLETS.

Signature

Print Name

Date

Exhibit G
Business Associate Agreement

This Qualified Service Organization/Business Associate Addendum ("Addendum") supplements and is made a part of the services agreement ("Agreement") by and between County of Sonoma ("County") and The Act 1 Group, Inc. dba ATIMS ("Qualified Service Organization/Business Associate").

RECITALS

WHEREAS, County is a Hybrid Entity as defined under 45 Code of Federal Regulations ("CFR") Section 164.103;
WHEREAS, The Act 1 Group, Inc. dba ATIMS is a Qualified Service Organization/Business Associate (QSO/BA) as defined under 45 CFR Section 160.103;
WHEREAS, County wishes to disclose certain information to QSO/BA pursuant to the terms of Addendum, some of which information may constitute Protected Health Information ("PHI"), including electronic Protected Health Information ("ePHI");
WHEREAS, County and QSO/BA intend to protect the privacy and provide for the security of PHI, including ePHI, disclosed to QSO/BA pursuant to Addendum in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104 191 ("HIPAA"), regulations promulgated thereunder by the U.S. Department of Health and Human Services, and other applicable laws; and
WHEREAS, as part of the HIPAA Regulations, the Privacy Rule and Security Rule require County to enter into a contract containing specific requirements with QSO/BA prior to the disclosure of PHI, including ePHI, as set forth in, but not limited to, 45 CFR Sections 164.502(e), 164.504(e), and 164.308(b)(1) and contained in Addendum.
NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to Addendum, the parties agree as follows:

- Definitions
  Terms used, but not otherwise defined, in Addendum shall have the same meaning as those terms in the HIPAA Regulations as set forth at 45 CFR Sections 160.103, 164.304, and 164.501.

  A. HIPAA Regulations
  "HIPAA Regulations" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules as set forth at 45 CFR Part 160 and Part 164.

  B. Breach
  "Breach" shall mean the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 CFR Part 164 Subpart E and that compromises the security or privacy of PHI as defined at 45 CFR Section 164.402.

  C. Business Associate
  "Business Associate" shall have the same meaning as the term "Business Associate" as set forth at 45 CFR Section 160.103.

  D. Covered Entity
  "Covered Entity" shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 CFR Section 160.103. For purposes of this Addendum, this term is intended to mean the County of Sonoma.

  E. Data Aggregation
  "Data Aggregation" shall have the same meaning as the term "Data aggregation" as set forth at 45 CFR Section 164.501.

  F. Designated Record Set
  "Designated Record Set" shall have the same meaning as the term "designated record set" as set forth at 45 CFR Section 164.501.

  G. Disclosure
  "Disclosure" shall mean the release of, transfer of, provision of access to, or divulging in any manner information outside the entity holding the information in accordance with 45 CFR Section 160.103.

  H. Health Care Operations
  "Health Care Operations" shall have the same meaning as "Health care operations" as set forth at 45 CFR Section 164.501.

  I. Individual

"Individual" shall have the same meaning as the term "Individual" as set forth at 45 CFR Section 164.501, except that the term "Individual" as used in this Addendum shall also include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

J. Minimum Necessary
"Minimum Necessary" shall mean the minimum amount of PHI necessary for the intended purpose, as set forth at 45 CFR Sections 164.502(b) and 164.514(d): Standard: Minimum Necessary.

K. Part 2 Regulations
"Part 2 Regulations" shall mean the Confidentiality of Substance Use Disorder Patient Records regulations as set forth at 42 CFR Part 2.

L. Patient Identifying Information
"Patient Identifying Information" shall have the same meaning as the term "patient identifying information" as set forth at 42 CFR Section 2.11, except the term "Patient Identifying Information" as used in this Addendum may also include Protected Health Information.

M. Privacy Rule
"Privacy Rule" shall mean the HIPAA Standards for Privacy of Individually Identifiable Health Information as set forth at 45 CFR Part 160 and 45 CFR Part 164 Subparts A and E.

N. PHI
"PHI" shall have the same meaning as the term "protected health information" as set forth at 45 CFR Section 160.103, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by QSO/BA on behalf of Covered Entity.

O. Protected Health Information
"Protected Health Information" shall have the same meaning as the term "protected health information" as set forth at 45 CFR Section 160.103, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by QSO/BA on behalf of Covered Entity, and may include Patient Identifying Information.

P. Protected Information
"Protected Information" shall mean "Protected Health Information" and "Patient Identifying Information."

Q. Qualified Service Organization
"Qualified Service Organization" shall have the same meaning as the term "qualified service organization" as set forth at 42 CFR Part 2 Section 2.11.

R. Required by Law
"Required by law" shall have the same meaning as the term "required by law" as set forth at 45 CFR Section 164.103.

S. Secretary
"Secretary" shall mean the Secretary of the United States Department of Health and Human Services ("DHHS") or his/her designee.

T. Security Incident
"Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of personally identifiable information. A Security Incident includes the attempted or successful unauthorized access, use, disclosure, modification, or destruction of or interference with systems operations in an information system which processes PHI that is under the control of Covered Entity or QSO/BA of Covered Entity, but does not include minor incidents that occur on a daily basis, such as scans, "pings", or unsuccessful random attempts to penetrate computer networks or servers maintained by QSO/BA.

U. Security Rule
"Security Rule" shall mean the HIPAA Security Standards for the Protection of ePHI as set forth at 45 CFR Part 160 and 45 CFR Part 164 Subparts A and E.

V. Subcontractor
"Subcontractor" shall mean a subcontractor of QSO/BA that creates, receives, maintains, or transmits PHI on

behalf of QSO/BA.

W. Unsecured PHI
"Unsecured PHI" shall have the same meaning as the term "unsecured protected health information" as set forth at 45 CFR Section 164.402, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by QSO/BA on behalf of Covered Entity.

X. Use
"Use" shall mean, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information in accordance with 45 CFR Section 160.103.

- Obligations of QSO/BA
QSO/BA acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any Protected Information received from County, QSO/BA is fully bound by the HIPAA Regulations and the Part 2 Regulations; and that QSO/BA (including its subcontractors) may be held directly liable for and subject to penalties for failure to comply. To the extent QSO/BA is to carry out one or more of County's obligations under of 45 CFR Part 164 Subpart E of the Privacy Rule, QSO/BA agrees to comply with the requirements of 45 CFR Part 164 Subpart E that apply to County in the performance of such obligations.

- Use or Disclosure of Protected Health Information
Except as otherwise provided in Addendum, QSO/BA shall use and/or disclose Protected Information only as necessary to perform functions, activities, or services documented in the Scope of Work (Exhibit A) of this Agreement for or on behalf of County, as specified in Addendum, provided that such use and/or disclosure does not violate the 42 CFR Part 2 Regulations or the HIPAA Regulations. QSO/BA agrees not to further use or disclose Protected Information other than as permitted or required by Addendum or by law. QSO/BA must make reasonable efforts to limit Protected Information to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request. The uses of Protected Information may not exceed the limitations applicable to County under the 42 CFR Part 2 and HIPAA Regulations.

- Prohibited Uses and Disclosures
A. Contractor shall not disclose Department PHI about an individual to a health plan for payment or health care operations purposes if the Department PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. Section 17935(a) and 45 CFR Section 164.522(a).
B. Contractor shall not directly or indirectly receive remuneration in exchange for PHI.

- Judicial Proceedings
QSO/BA agrees to resist any efforts in judicial proceedings to obtain access to Patient Identifying Information except as expressly provided for in the regulations governing the Part 2 Regulations.

- Designation of a Privacy Officer and a Security Officer
A. Contractor shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of the HIPAA Security Rule (45 CFR Part 164 Subpart C)
B. Contractor shall designate a Privacy Officer to oversee its information privacy program who shall be responsible for carrying out the requirements of the HIPAA Privacy Rule (45 CFR Part 164 et. seq.)
C. The individual designated to the above roles may be the same individual so long as they are qualified and able to effectively perform the duties of both designations.

- Safeguarding Protected Health Information
QSO/BA shall use appropriate safeguards to prevent the use or disclosure of Protected Information other than as provided for by Addendum. QSO/BA shall implement administrative, physical, and technical safeguards and shall comply with of 45 CFR Part 164 Subpart C with respect to electronic Protected Information that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic Protected Information created, received, maintained, or transmitted on behalf of County and prevent the use or disclosure of Protected Information other than as provided for by Agreement.

A. Encryption Requirements for Transmission and Storage of Electronic Data. All Protected Information transmitted to QSO/BA by County, and/or for or on behalf of County by QSO/BA, and/or to County by QSO/BA shall be provided or transmitted using encryption methods which render such Protected Information unusable,

unreadable, or indecipherable by unauthorized persons. All ePHI stored by Business Associate on electronic media shall be protected using encryption methods which render such ePHI unusable, unreadable, or indecipherable by unauthorized persons. Encryption of ePHI in transit or at rest shall use a technology or methodology set forth by the Secretary in the guidance issued under Section 13402(h)(2) of Public Law 111-5, and in accordance with the National Institute of Standards Technology (NIST) and Standards and Federal Information Processing Standards (FIPS), as applicable.

B. Destruction of Protected Information on paper, film, or other hard copy media must involve either shredding or otherwise destroying the Protected Information so that it cannot be read or reconstructed.

C. Should any employee or subcontractor of QSO/BA have direct, authorized access to County computer systems that contain Protected Information, QSO/BA shall immediately notify County of any change of such personnel (e.g., employee or subcontractor termination, or change in assignment where such access is no longer necessary) in order for County to disable the previously authorized access.

- Notification of Breach, Unauthorized Use or Improper Disclosure
  QSO/BA must notify County in writing of any access, use, or disclosure of Protected Information not permitted or provided for by Addendum and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations of which Business Associate becomes aware. A breach or unauthorized access, use, or disclosure shall be treated as discovered by QSO/BA the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have been known, to QSO/BA or to any person, other than the individual committing the unauthorized disclosure, that is an employee, officer, subcontractor, agent, or other representative of QSO/BA.

  A. Notification must be made as soon as practicable, but not later than 24 hours after discovery, by telephone call to 707-565-5703 plus e-mail to:
     DHS-Privacy&Security@sonoma-county.org , and will include:
     1) The identification of each Individual whose PHI has been, or is reasonably believed by QSO/BA to have been, accessed, acquired, used, or disclosed; and
     2) A description of any remedial action taken or proposed to be taken by QSO/BA.

  B. QSO/BA must provide a complete report of the investigation to the County Privacy and Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the “Privacy Incident Report” form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the County requests information in addition to that listed on the “Privacy Incident Report” form, Contractor shall make reasonable efforts to provide the County with such information.

  C. QSO/BA must mitigate any harm that results or may result from the breach, security incident, or unauthorized access, use, or disclosure of unsecured PHI by QSO/BA or its employees, officers, subcontractors, agents, or other representatives.

  D. Following a breach or unauthorized access, use, or disclosure of unsecured PHI, QSO/BA agrees to take any and all corrective action necessary to prevent recurrence, to document any such corrective action, and to make this documentation available to County.

- Agents and Subcontractors of QSO/BA
  In accordance with 45 CFR Sections 164.502(e)(1)(ii) and 164.308(b)(2), and to the extent that QSO/BA uses any agent, including a subcontractor, to which QSO/BA provides PHI received from, created by, maintained by, or received by QSO/BA on behalf of County, QSO/BA shall execute an agreement with such agent or contractor containing a requirement to ensure compliance with the same restrictions and conditions that apply through Addendum to QSO/BA with respect to PHI.

- Access to Protected Health Information
  At the request of County, and in the time and manner designated by County, QSO/BA shall provide access to PHI in Designated Record Set to an Individual or County to meet the requirements of 45 CFR Section 164.524, and Ca. Health & Safety Code 123100 et. seq.

- Amendments to Protected Information
  QSO/BA shall make any amendment(s) to Protected Information as directed or agreed to by County, or shall take other measures necessary to satisfy County's obligations under 45 CFR Section 164.526.

- Accounting of Disclosures
  QSO/BA shall document and make available such disclosures of PHI and information related to such disclosures as would be required for County to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

- Records Available to County, State, and Secretary
  QSO/BA shall make available internal practices, books, and records related to the use, disclosure, and privacy protection of PHI received from County, or created, maintained, or received by QSO/BA on behalf of County, to County, State, or the Secretary for the purposes of investigating or auditing QSO/BA's compliance with the HIPAA Regulations in the time and manner designated by County, State, or Secretary.

- Return or Destruction of Protected Health Information

  A. Upon termination of Addendum for any reason, QSO/BA shall:
     1) Return all PHI received from County; return all PHI created, maintained or received by QSO/BA on behalf of County; and return all PHI required to be retained by the HIPAA Regulations; OR:
     2) at the discretion of County, destroy all PHI received from County, or created, maintained, or received by QSO/BA on behalf of County. Destruction of PHI on paper, film, or other hard copy media must involve shredding or otherwise destroying the PHI in a manner which will render the PHI unreadable, undecipherable, or unable to be reconstructed. QSO/BA shall certify in writing that such PHI has been destroyed.

  B. In the event QSO/BA determines that returning or destroying PHI is not feasible, QSO/BA shall provide County notification of the conditions that make return or destruction not feasible. QSO/BA shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as QSO/BA maintains such PHI.

- Data Aggregation
  QSO/BA may provide data aggregation services related to the health care operations of County as permitted by 45 CFR Section 164.504(e)(2)(i)(B).

- Other Applicable Laws
  QSO/BA shall comply with all other applicable laws to the extent that such state confidentiality laws are not preempted by the HIPAA Regulations or the Part 2 Regulations.

- Penalties/Fines for Failure to Comply with HIPAA
  QSO/BA shall pay any penalty or fine assessed against Covered Entity arising from QSO/BA's failure to comply with the obligations imposed by HIPAA.

- Training of Employees and Enforcement of Requirements
  QSO/BA shall train and use reasonable measures to ensure compliance with the requirements of this QSO/BA Agreement by employees who assist in the performance of functions or activities on behalf of County under this Contract and use or disclose protected information; and discipline employees who intentionally violate any provisions.

- Amendments to Addendum
  No amendment of Addendum shall be effective unless and until such amendment is evidenced by a writing signed by the parties. County and QSO/BA agree to take such action as is necessary to amend Addendum as required for County to comply with the requirements of the HIPAA Regulations. However, any provision required by HIPAA Regulations to be in Addendum shall bind the parties whether or not provided for in Addendum.

- Termination of Addendum
  If QSO/BA should fail to perform any of its obligations hereunder, or materially breach any of the terms of Addendum, County may terminate Addendum immediately upon provision of notice stating the reason for such termination to QSO/BA. County, within its sole discretion, may elect to give QSO/BA an opportunity to cure such breach.

- Material Breach
  A breach by QSO/BA or any of its agents or subcontractors of any provision of Addendum, as determined by County, shall constitute a material breach of Addendum and shall provide grounds for immediate termination of Addendum.

- Indemnification
  QSO/BA agrees to accept all responsibility for loss or damage to any person or entity, including County, and to

indemnify, hold harmless, and release County, its officers, agents, and employees from and against any actions, claims, damages, liabilities, disabilities, or expenses that may be asserted by any person or entity, including QSO/BA, that arise out of, pertain to, or relate to QSO/BA's or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under Agreement. QSO/BA agrees to provide a complete defense for any claim or action brought against County based upon a claim relating to such QSO/BAs' or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under Agreement. QSO/BAs' obligations under Article 5 (Indemnification) apply whether or not there is concurrent negligence on County's part, but to the extent required by law, excluding liability due to County's conduct. County shall have the right to select its legal counsel at QSO/BA's expense, subject to QSO/BA's approval, which shall not be unreasonably withheld. This indemnification obligation is not limited in any way by any limitation on the amount or type of damages or compensation payable to or for QSO/BA or its agents under workers' compensation acts, disability benefits acts, or other employee benefit acts.

Part II: Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA: (Applies to all contractors)

1. Recitals

A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the County is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:

1) The California Information Practices Act of 1977 (California Civil Code §§1798 et seq.).

2) The Agreement between the Social Security Administration (SSA) and the County, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA, is attached to this Exhibit as Attachment B and is hereby incorporated in this Agreement.

B. The purpose of this Exhibit, Part II is to set forth Contractor's privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for or on behalf of County pursuant to this Agreement. Specifically, this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in this Exhibit, Part I of this Agreement, the HIPAA Business Associate Addendum.

C. The IEA Agreement referenced in A.2) above requires the County to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from County that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security Procedures, F. Contractor/Agent Responsibilities, and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides County data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.

D. The terms used in this Exhibit, Part II, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and Agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions

A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.

B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code § 1798.29(d).

C. Confidential Information shall mean information that is exempt from disclosure under the provisions of the

California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws

D. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS). https://www.ssa.gov/dataexchange/documents/CMPPA%20State%20Model.pdf

E. "County PI" shall mean Personal Information, as defined below, accessed in a database maintained by the County, received by Contractor from the County or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the County.

F. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS). https://www.ssa.gov/dataexchange/documents/IEA(F)%20State%20Level.pdf

G. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29(e) whose unauthorized access may trigger notification requirements under Civil Code § 1709.29. For purposes of this provision, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

H. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

I. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code § 1798.3(a).

J. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

K. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

L. Sensitive Information shall mean information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

3. Terms of Agreement

A. Permitted Uses and Disclosures of County PI and PII by Contractor

Except as otherwise indicated in this Exhibit, Part II, Contractor may use or disclose County PI only to perform functions, activities or services for or on behalf of the County pursuant to the terms of this Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the County.

B. Responsibilities of Contractor

Contractor agrees:

1) **Nondisclosure**. Not to use or disclose County PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.

- The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).

- The Contractor and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Contractor's obligations under this Agreement.

- The Contractor and its employees, agents, or subcontractors shall promptly transmit to the County Program Contract Manager all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.

- The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than County without prior written authorization from the County Program Contract Manager, except if disclosure is required by State or Federal law.

2) **Safeguards**. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of County PI and PII, to protect against anticipated threats or hazards to the security or integrity of County PI and PII, and to prevent use or disclosure of County PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of Section 3, Security, below. Contractor will provide County with its current policies upon request.

3) **Security**. Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/orPI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

a) Complying with all of the data system security precautions listed in Part IV of this Special Terms and Conditions Document, Contractor Data Security Requirements; and

b) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

c) If the data obtained by User(s) from County includes PII, User(s) shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement (IEA), which are attached as Attachment B and are incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide County PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide County PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.

4) **Mitigation of Harmful Effects**. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PI or PII by Contractor or its subcontractors in violation of this Exhibit, Part II.

5) **Contractor's Agents and Subcontractors**. To impose the same restrictions and conditions set forth in this Exhibit, Part II on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of County PI or PII to the subcontractor.

6) **Availability of Information to County**. To make PI and PII available to the County for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of County PI and PII. If Contractor receives County PII, upon request by County, Contractor shall provide County with a list of all employees, contractors and agents who have access to County PII, including employees, contractors and agents of its subcontractors and agents.

7) **Cooperation with County.** With respect to County PI, to cooperate with and assist the County to the extent necessary to ensure the County's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of County PI, correction of errors in County PI, production of County PI, disclosure of a security breach involving County PI and notice of such breach to the affected individual(s).

8) **Breaches and Security Incidents**. During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

a) **Initial Notice to the County**. (1) To notify the County **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured County PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving County PII. (2) To notify the County **within 24 hours (1 hour if SSA data) by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of County PI or PII in violation of this Agreement or this Exhibit, Part I, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

b) Notice shall be provided to the County Privacy and Security Officer. If the incident occurs after business hours or on a weekend or holiday andinvolves electronic County PI or PII, notice shall be provided by calling the County Privacy and Security Officer. Notice shall be made using the County "Privacy Incident Report" form.

c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PHI , Contractor shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

d) **Investigation and Investigation Report**. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at the time, to the County Privacy and Security Officer.

e) **Complete Report**. To provide a complete report of the investigation to the County Privacy and Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper

use or disclosure. If the County requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the County with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the County may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The County will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

f) **Responsibility for Reporting of Breaches**. If the cause of a breach of County PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, § 1798.29(a) – (d) and as may be required under the IEA. Contractor shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The County Privacy and Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The County will provide its review and approval expeditiously and without unreasonable delay. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the County in addition to Contractor, Contractor shall notify the County, and the County and Contractor may take appropriate action to prevent duplicate reporting.

g) **County Contact Information**. To direct communications to the above referenced County staff, the Contractor shall initiate contact as indicated herein. The County reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

Sonoma Co. Privacy Officer: 1450 Neotomas Ave. Suite 200, Santa Rosa, C 95405; 707-565-5703; DHS-Privacy&Security@Sonoma-County.org

Part III: Miscellaneous Terms and Conditions (Applies to all Contractors)

1. Disclaimer

The County makes no warranty or representation that compliance by Contractor with this Exhibit, HIPAA or the HIPAA regulations will be adequate or satisfactory for Contractor's own purposes or that any information in Contractor's possession or control, or transmitted or received by Contractor, is or will be secure from unauthorized use or disclosure. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of the County PHI.

2. Amendment

A. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit maybe required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. The County may terminate this Agreement upon thirty (30) days written notice in the event:

1) Contractor does not promptly enter into negotiations to amend this Exhibit when requested by the County pursuant to this section; or

2) Contractor does not enter into an amendment providing assurances regarding the safeguarding of County PHI that the County deems necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

3. Judicial or Administrative Proceedings

Contractor will notify the County if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. The County may terminate this Agreement if Contractor is found guilty of a criminal violation of HIPAA. The County may terminate this Agreement if a finding or stipulation that the Contractor has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Contractor is a party or has been joined. County will consider the nature and seriousness of the violation in deciding whether or not to terminate the Agreement.

4. Assistance in Litigation or Administrative Proceedings

Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to the County at no cost to the County to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the County, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.

5. No Third-Party Beneficiaries

Nothing express or implied in the terms and conditions of this Exhibit is intended to confer, nor shall anything herein confer, upon any person other than the County or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

6. Interpretation

The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, and the HIPAA regulations. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.

7. Conflict

In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

8. Regulatory References

A reference in the terms and conditions of this Exhibit to a section in the HIPAA regulations means the section as in effect or as amended.

9. Survival

The respective rights and obligations of Contractor under Section 3, Item D of this Exhibit, Part I, Responsibilities of Contractor, shall survive the termination or expiration of this Agreement.

10. No Waiver of Obligations

No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

11. Audits, Inspection and Enforcement

From time to time, and subject to all applicable federal and state privacy and security laws and regulations, the County may conduct a reasonable inspection of the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit. The

fact that the County inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit. The County's failure to detect a non-compliant practice, or a failure to report a detected non-compliant practice to Contractor does not constitute acceptance of such practice or a waiver of the County's enforcement rights under this Agreement, including this Exhibit.

12. Due Diligence

Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit.

13. Term

The Term of this Exhibit shall extend beyond the termination of the Agreement and shall terminate when all County PHI is destroyed or returned to the County, inaccordance with 45 C.F.R. § 164.504(e)(2)(ii)(I), and when all County PI and PII is destroyed in accordance with Attachment A.

14. Effect of Termination

Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all County PHI, PI and PII that Contractor still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify the County of the conditions that make the return or destruction infeasible, and the County and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of this Exhibit to such County PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to County PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

Part IV: Contractor Data Security Requirements

1. General Controls

Contractor shall preserve and shall ensure that its sub-consultants or vendors preserve, the confidentiality, integrity, and availability of County data with administrative, technical and physical measures that conform to generally recognized industry standards and best practices that the selected firm then applies to its own processing environment. Maintenance of a secure processing environment includes, but is not limited to, the timely application of patches, fixes and updates to operating systems and applications as provided by Contractor and/or its sub-consultants or vendors. Contractor agrees to, and shall ensure that its sub-consultants or venders, comply with County's current and future information security policies, standards, procedures, and guidelines.

2. Designation of Individual(s) Responsible for information Privacy and Security

A. Security Officer:

Contractor shall designate a qualified individual, (HIPAA Security Officer), to implement and oversee its data security program. The individual shall be responsible for, and knowledgeable about, carrying out the requirements of this Special Terms and Conditions Exhibit, ensuring Contractor compliance with all provisions of the HIPAA Security Rule (45 CFR 164.300 et. seq.), and for communicating about security matters with the County.

B. Privacy Officer:

Contractor shall designate a qualified individual, (HIPAA Privacy Officer), to implement and oversee its information privacy program. The individual shall be responsible for, knowledgeable about, and trained in, carrying out the requirements of this Special Terms and Conditions Exhibit, ensuring Contractor compliance with all applicable state and federal information privacy laws (including but not limited to HIPAA, WIC 5328, 42 CFR Part 2, California Medical Information Act, etc.), and for communicating about privacy and security matters with the County.

C. The individual designated to the above roles may be the same individual so long as they are qualified and able to

effectively perform the duties of both designations.

3. Personnel Controls

A. **Employee Training**. All workforce members who assist in the performance of functions or activities on behalf of the County, or access or disclose County PHI or PI must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.

B. **Employee Discipline**. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. **Confidentiality Statement**. All persons that will be working with County PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to County PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for County inspection for a period of six (6) years following termination of this Agreement.

D. **Background Check**. Before a member of the workforce may access County PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

4. Technical Security Controls

A. **Workstation/Laptop encryption**. All workstations and laptops that store County PHI or PI either directly or temporarily must be encrypted using a FIPS140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the County Privacy and Security Office.

B. **Server Security**. Servers containing unencrypted County PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. **Minimum Necessary**. Only the minimum necessary amount of County PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. **Removable media devices**. All electronic files that contain County PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

E. **Antivirus software**. All workstations, laptops and other systems that process and/or store County PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. **Patch Management**. All workstations, laptops and other systems that process and/or store County PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory

controls implemented to minimize risk, where possible.

G. **User IDs and Password Controls**. All users must be issued a unique user name for accessing County PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of charactersfrom at least three of the following four groups from the standard keyboard:

1) Upper case letters (A-Z)
2) Lower case letters (a-z)
3) Arabic numerals (0-9)
4) Non-alphanumeric characters (punctuation symbols)

H. **Data Destruction**. When no longer needed, all County PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the County Privacy and Security Office.

I. **System Timeout**. The system providing access to County PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

J. **Warning Banners**. All systems providing access to County PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

K. **System Logging**. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for County PHI or PI, or which alters County PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If County PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

L. **Access Controls**. The system providing access to County PHI or PI must use role-based access controls for all user authentications, enforcing the principle of least privilege.

M. **Transmission encryption**. All data transmissions of County PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing County PHI can be encrypted. This requirement pertains to any type of County PHI or PI in motion such as website access, file transfer, and E-Mail.

N. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting County PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

5. Audit Controls

A. **System Security Review**. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing County PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

B. **Log Reviews**. All systems processing and/or storing County PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

C. **Change Control**. All systems processing and/or storing County PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and

availability of data.

D. **Random Audits**. Contractor will accommodate and upon reasonable notice by Sonoma County, work with Sonoma County and/or its subcontractors to submit to a random information security audit. This is to ensure that Contractor's and/or vendor's information security practices or standards comply with Sonoma County's information security policies, standards, procedures and guidelines. Contractor shall ensure that its sub-consultants or vendors comply with this requirement.

6. Business Continuity / Disaster Recovery Controls

A. **Emergency Mode Operation Plan**. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of County PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

B. **Data Backup Plan**. Contractor must have established documented procedures to backup County PHI to maintain retrievable exact copies of County PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore County PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of County data.

7. Paper Document Controls

A. **Supervision of Data**. County PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. County PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. **Escorting Visitors**. Visitors to areas where County PHI or PI is contained shall be escorted and County PHI or PI shall be kept out of sight while visitors are in the area.

C. **Confidential Destruction**. County PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. **Removal of Data**. Only the minimum necessary County PHI or PI may be removed from the premises of the Contractor except with express written permission of the County. County PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of the same Contractor's locations.

E. **Faxing**. Faxes containing County PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. **Mailing**. Mailings containing County PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of County PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the County to use another method is obtained.

Part V: Provisions for Access to County Electronic Health Records System
(Applies to contractors that have access to County E.H.R. system)

1. General Controls

AGREEMENTS AND CONDITIONS OF ACCESS AND USE In consideration for use of the Department of Health Services (DHS) Electronic Health Record system ("EHR"), User agrees to the following terms and conditions:

A. Contractor shall only use the EHR system to support clients served pursuant to a contract with the County.

B. Contractor and Contractor staff shall only access the EHR and Protected Health Information for the purpose of providing healthcare services.

C. Contractor shall ensure that staff will not use or disclose Protected Health Information other than as permitted or as required by law or this Agreement.

D. Contractor shall ensure that staff will not share or give authentication credentials, such as a USERID or password, to any other individual, or fail to take appropriate measures to safeguard their authentication credentials.

E. Contractor shall ensure that all staff with EHR access shall be trained on (i) the use of the EHR system; (ii) safeguards necessary to protect the EHR system, and (iii) the proper use/disclosure of information stored in the EHR system.

F. Contractor shall ensure that all staff with access to the EHR system sign a confidentiality agreement stating they will maintain confidentiality of protected information maintained in the EHR System. This agreement may be combined with other required confidentiality agreements.

G. Within 24 hours of discovery, Contractor shall report to DHS Privacy and Security Officer any use or disclosure of Protected Health Information which would violate State/federal regulations or the terms of this Agreement.

H. Contractor shall notify County of staff enrollment, staff changes job duties/credentialling, or staff separation from employment within 24 hours of the staff change using the form provided by the County.

I. County shall be responsible for enrollment of new staff into the EHR system, and adjustments to staff's level of access when staff changes job duties/credentialling or staff is separated from employment.

J. Contactor shall comply with all other information privacy and security provisions as articulated in this Agreement and exhibits.

K. If any use or disclosure of Protected Health Information by Contractor or Contractor's agents, staff, subcontractors, or invitees violates State/Federal regulations or the terms of this Agreement, Contractor agrees to accept all responsibility in accordance with Provision 19 (Indemnification) of this Agreement.

Exhibit H

County Policy 9-2 Information Technology Use and Security Policy

https://sonomacounty.ca.gov/administrative-support-and-fiscal-services/human-resources/employee-resources/administrative-policy-manual/9-2-it-use-and-security-policy

Exhibit I

County Policy 9-4 Information Technology Professionals Policy

https://sonomacounty.ca.gov/administrative-support-and-fiscal-services/human-resources/employee-resources/administrative-policy-manual/9-4-information-technology-professionals-policy

Exhibit J

County Policy 9-6 Information Technology Artificial Intelligence (AI) Policy

https://sonomacounty.ca.gov/administrative-support-and-fiscal-services/human-resources/employee-resources/administrative-policy-manual/ 9-6-information-technology-artificial-intelligence-(ai)-policy

TECHNOLOGY
SERVICES AND SOLUTIONS

Inmate Records Information System
Statement of Work

Table of Contents

A) OVERVIEW

Purpose

This Statement of Work ("SOW") sets forth the professional services (collectively, the "Services") to be provided by The Act 1 Group, Inc. (DBA ATIMS) to Sonoma County ("County") to provide a Jail Management System (JMS), implement the JMS, bring the Sonoma County Sheriff's Office ("SO") live on the new JMS, and provide production support for the JMS.

This SOW is a fixed price arrangement for ATIMS to provide their Software as a Service (SaaS) model JMS software, professional services, and deliverables defined herein, to implement the JMS after which upon Go Live ATIMS will continue to support the County with JMS Production Support ("Maintenance") and ongoing hosting services ("Hosting") for a period of five years with the option to extend for two (2) additional 2-year periods unless terminated earlier or otherwise amended,

The Statement of Work ("SOW") defines the products and services, process, principal activities, artifacts, and responsibilities of ATIMS and the County for the implementation of the County's JMS including roles, project management approach, requirements, phases, milestones, deliverables, and activities/tasks.

The Statement of Work ("SOW") is incorporated into and governed by the contract between the County and ATIMS ("Agreement"). Elements of the SOW may be clarified or modified by the County, and the SOW may be updated in writing as required throughout the life of the JMS project and implemented through a Change Order or amendment to the Agreement.

The purpose of this project is to provide the County with a new, completely integrated, solution that will fully meet or exceed all of the County's requirements as set forth in the County's Request for Proposals as agreed to in the ATIMS proposal and/or this SOW and all additional requirements identified and agreed to by ATIMS and the County and documented in a formal Change Order, Contract Amendment, or other appropriate documentation.

The project will be considered successful and complete when the new JMS application has been placed into production, all functionality has been successfully implemented and tested per the SOW and related Deliverable Expectation Documents (DED), and the County has accepted the application (See Section C: Acceptance Process, Final Acceptance).

This SOW incorporates the following documents:

Exhibit	Type
Appendix A	Definitions and Terms
Appendix B	Deliverable Summary
Appendix C	Requirement Modifications
Appendix D	Requirement Fees
Attachment 1	Deliverable Expectation Document
Attachment 2	Deliverable Notice
Attachment 3	Acceptance Notice

Attachment 4	Change Request Form
Attachment 5	Interface Control Document (ICD)

The SOW and subsequent change orders shall govern the specific milestones and deliverables of the JMS project.

Incorporated into the SOW by reference is:

- The County's Request for Proposal (RFP) and related documents released as part of the RFP
- The ATIMS Proposal and related documents submitted as part of the Proposal

Background

The County of Sonoma (County) is seeking a comprehensive, integrated, and modern jail management system (JMS) for the Office of the Sheriff (Sheriff's Office, SO) to replace various disparate and outdated systems, to increase the safety of inmates and staff, and to enhance jail operations and inmate management.

The jail management solution will be used to perform day-to-day operational criminal offender processing. The solution will replace the jail related portion of the County's legacy Integrated Justice System (IJS) system.

IJS supports County justice agencies and the local Superior Court and provides query and reporting capabilities to over 60 local, regional, state, and federal agencies. The eventual replacement of IJS will bring the opportunity for all criminal justice partners to seek more modern, updated, and flexible systems that can integrate with their local criminal justice partners and grow to meet changing business needs. A new JMS is a core component of the County's modernization plan.

The JMS must tightly integrate with approximately several other core applications, used within the Sheriff's Office and other County departments and external agencies, such as the Sonoma County Superior Court. The JMS will also replace many manual and paper-based processes which have previously limited modernization activities due to the County's reliance on IJS and available functionality.

Stakeholders

The County of Sonoma

The County of Sonoma has approval authority over the project as a whole.

Sonoma County Sheriff's Office (SO)

The Sonoma County Sheriff's Office has primary and final authority on decisions relating to the project scope, timeframe, budget, and change orders, and will determine whether acceptance criteria for deliverables have been satisfied. The SO also has a responsibility to provide necessary project resources and project management, to participate in requirements confirmation, and conduct user acceptance testing.

The Sheriff's Office currently operates two jail sites.

- The Main Adult Detention Facility (MADF) is a medium to maximum security facility designed to house

both pre-trial and sentenced inmates with a capacity of approximately 900 inmates.

• The North County Detention Facility (NCDF) is a medium security facility with a capacity of approximately 250 inmates. NCDF is currently on standby to handle overflow from MADF.

The Sheriff's Office, as the primary user of the JMS, will provide subject matter expertise, and work closely with ATIMS during the implementation.

ATIMS Jail Management System is licensed based on active inmate population count, not on number of users or devices. See Payment and Fee Schedule in Exhibit B for active inmate population cap and fees for sustained increases of inmate population.

Technical Services Bureau Information Technology Unit
The Technology Services Bureau is responsible for information and technology systems planning, development, acquisition, business analysis, implementation, support, and maintenance to the Sheriff's Office departments.

ATIMS
ATIMS (previously dba DSSI), is based in Chatsworth, CA (Los Angeles County). Focused on jail management systems since 1999, ATIMS is a division of the ActOne Group, Inc., privately owned by the Howroyd family. Brett Howroyd is the President of ActOne and all subsidiaries, including ATIMS, and Felix Rabinovich serves as Vice President of ATIMS.

ATIMS will provide their JMS system and all professional services and deliverables described in the Statement of Work. ATIMS will work directly with the County in the management and execution of the Statement of Work.

Additional Stakeholders
Additional County stakeholder agencies and departments include:

- Sonoma County Courts
- County of Sonoma Health Services
- Pretrial Services
- Public Defender's Office and Alternate Defenders Office
- District Attorney
- Probation
- Facilities and Fleet

Cooperation
Implementation of the JMS will involve ATIMS staff and County staff, from both the Sheriff's Office and Technology Services and Solutions department, working cooperatively in partnership to achieve the project objectives.

Objectives

The County's primary objectives in implementing the ATIMS JMS, by which the success of this JMS

implementation project will be measured are noted in detail in the RFP and include:

1) **Adopt Jail Management Operational Best Practices:** Wherever practical, the County intends to use the functionality, workflows, and automation capabilities provided by the JMS to achieve County and nationally recognized operational best practices.

2) **Fully Replace Key Legacy Systems / Functionality:** Following implementation of the new JMS, the County's intent is that there would not be a need for Corrections Staff to utilize any part of the legacy CJIC system to support jail intake or daily jail operation as well as other systems that the JMS will replace. The County seeks to implement a "state-of-the-art" jail management solution that will satisfy all the County's current requirements and be easy to maintain, easy and inexpensive to upgrade, and can expand to satisfy future needs for additional functionality and/or processing capacity.

3) **Replace Most Jail Intake and Jail Operations Manual/Paper-based Processes:** A majority of Sheriff Office corrections-related manual and paper-based processes are expected to be made obsolete and replaced with the new JMS.

4) **Create a Fully Integrated Jail Management Environment:** The JMS is expected to have multiple integrations as part of its overall operation. The new JMS is expected to integrate with a variety of systems, including but not limited to:

    a. Critical Jail Support Systems (e.g., commissary, law enforcement criminal record/offender registry systems, internal affairs and use of force investigation systems, inmate assessment and classification systems, and inmate tracking system).

    b. Enabling Jail Technologies (e.g., fingerprint capture (Automated Fingerprint Identification System), signature capture, mugshot capture, document scanning/ storage, radio-frequency identification (RFID) scanning, and mobile devices).

    c. Various County and State Public Safety and Justice (PSJ) systems (e.g., Court Case Management System (CMS), District Attorney CMS, and Probation CMS); and

    d. Other internal or external systems (e.g., County's Electronic Health Record System, SLETS/CLETS Message Switch, National Law Enforcement Telecommunications System (NLETS), and Victim Notification System) and the Guardian RFID-based Inmate Tracking System (ITS).

5) **Employ a Modular System Architecture:** A modular design is required where components of the JMS system could be selectively utilized by the Sheriff's Office or by other justice partners without impact or degradation to the system. For example, law enforcement agencies (LEAs) who are not full JMS system users, can initiate the booking and intake process via a Custody Pre-Processing Portal (CPPP) which will interface with CJIC via the County's Information Sharing Environment (ISE).

6) **Develop Business Intelligence Capabilities:** Robust management and operational reporting are critical to the success of the new JMS. Management reporting built around intuitive data visualizations (charts, graphs, dashboards, and drilldowns) is required to provide real-time, accurate, and consumable information necessary to support internal decision-making at all levels (shift supervisors, facility leaders, specialty units, and command staff). Standard reports are needed to support day-to-day jail operations.

7) **Enable System Configurability and Flexibility:** A technology and application architecture that enables the ATIMS implementation staff to adapt and configure the proposed JMS solutions screens, workflows, dashboards, and business logic to align with County requirements -- to the greatest extent possible -- without requiring costly and time-consuming software code modifications or customizations. The Sheriff's Office IT personnel will be enabled to configure the system.

8) **Provide Multimedia Content:** Most of the County's existing JMS functions are supported by either "green screens," MS Access apps, macro-driven Excel workbooks, or manually handled paper forms. The County desires to replace as much of this as possible with modern, web based, mobile-capable solution that can display, process, and store both structured and unstructured data (videos, mugshots, scanned or electronically generated and signed forms) in a structured, but flexible database. The JMS solution should be able to be accessed by any authorized person, from any authorized location, using any authorized device.

9) **Develop Comprehensive Near Real-Time and Mobile Capabilities:** Currently, Corrections Officers (COs) and other staff carry clipboards containing paper forms that need to be filled out in writing for later entry into the system by jail staff. The new JMS will display real time as it is entered into the JMS and accessed via reporting, as well as near real-time data as agreed to by the County, including data from integrated systems. The JMS will also support the ability to easily enter data via a wireless-enabled laptop or tablet.

10) **Retain Historical Data**: The County will work with ATIMS to determine the best approach to migrate data from each existing system. At a minimum, historical data for current in-custody inmates will be migrated. Additionally, a process for migrating data related to specific types of offenders (e.g., high risk, gang/organized crime affiliations, frequent flyers, individuals with significant mental health and medical issues, etc.) will also need to be accommodated.

Systems Targeted for Replacement

The second objective of the Sheriff's Office is to "Fully Replace Key Legacy Systems/Functionality." The new JMS will replace the following systems and functionalities:

1) **IJS Functions**, management functions built into the legacy IJS system and targeted for replacement by the new JMS, include, but are not limited to:
    - Intake / Booking

- Inmate Housing / Bed Assignments
- Alternate Sentencing Program
- Release
- Reporting
- Court Schedule
- Administrative Booking (e.g., Court Services, Sentence Calculation, Bail Processing, Records Management)
- Classification
- Movement
- Programs
- Meals
- Transportation

Integrations

The future vision for the County is to modernize by seamlessly integrating the new JMS with other external systems and databases (e.g., the Court) so that inmate information needed by other organizations can be electronically shared in near real-time; sequential business processes that occur between organizations can be automatically triggered, delivered, and/or queued in relevant systems; and data can be easily exported for analysis, reporting, and decision making.

The JMS must tightly integrate with approximately 14 other core applications, some within the Sheriff's Office and some used by other County departments and external agencies, such as the Sonoma County Superior Court. These integrations will ensure that authorized personnel have access to essential information required to operate our jail facilities in a safe, secure, and efficient manner, and that other County agencies will have access to the information they need to perform their duties.

Interface requirements are detailed in the RFP Technical and Functional Requirements. and will be further detailed and documented during the course of the Project in the form of Interface Control Documents ("ICD").

As described in Track 3C: Analysis - Interfaces, integrations will utilize the County's Information Sharing Environment (ISE), an enterprise service bus architecture that provides a common method of interfacing County Public Safety and Justice applications with other systems. Exceptions allowing point to point integrations between data stores may be made with the County's approval.

Product Description

The ATIMS JMS consists of the following components and capabilities:

Modules and Functions

The ATIMS InCustody Jail Management System (JMS), is comprised of the following functional applications:

1. JMS – Jail Management System - The JMS is a completely configurable, state-of-the-art Jail Management System
2. PBPC – Pre-book and Probable Cause - The PBPC system allows for quick and accurate entry of arrest information and probable cause information. This information can be sent to Courts and District Attorney offices, as well as being used within the JMS. This eliminates multiple entries of the same data.
3. DIPL - Digital Photo Imaging & Lineup - The DIPL system is an investigative tool capable of creating 6- and 8-pack lineups, searching all person photos contained within the ATIMS product. These include mug shots, registrant pictures, scars, marks, and tattoos.
4. RIMS - Records Information Management System - The RIMS system is for the registration and management of court ordered registered offenders [not to be confused with Police Department RMS systems].
5. ADMIN – Administration Management - The ADMIN system is used for configuration and set up of all the above listed product.

ATIMS InCustody JMS includes the following modules:

- INMATE FILE (electronic file, includes all activities/records associated with inmate)
- SEARCH (inmate, booking, case, charge, records, photo, photo lineup)
- INTAKE (Prebook Queue/Detail, Temp Hold, Medical Pre-Screening, Inventory, Inmate Supply)
- BOOKING (Demographics, Charges, Bail, Attachments, Assessment, Housing, Calendar/Appointments, Transfer, Release, Supervisor monitor)
- CLASSIFY (Alerts/Flags hierarchy incl keep separates, forms, assessment calculations, programs/eligibility, waitlist, crews, furloughs, incidents, PREA, investigations, privileges)
- RECORDS (customized sentencing calculations, visitation, appointments, contact tracing, records inquiries, data handling, attachments, inmate release)
- PROPERTY (inventory, inmate supply, housing supply, issued property)
- FACILITY (counts, safety checks, housing dashboard, tracking, appointments, operations, visitation, pod management, movements/transportation, use of force, incident, grievance, requests, privileges, work crew, alternative requests, alerts, mail)
- MONITOR (status board, work queue, officer, timeline, today, personnel, housing dashboard, special handling, event subscriptions)
- PROGRAMS (case management, course management including active viewer, calendar, approved list, assignments, tracking, attendance)

- ALTERNATIVE CORRECTIONS (court commit, application, request, program, sites, site visit, transfer/movement, incident)
- MONEY (limited inmate ledger functionality, maintain balances, recommend interface to Inmate Trust Fund)
- MEDICAL (limited functionality to meet HIPPA requirements, includes pre-screen, charting, meds, forms, attachment, appointments and alerts)
- REPORTS (system, custom queues, user exports)
- REQUESTS (pending, assigned, search, status, can be interfaced to inmate self-service functionality for use by inmates and staff)

These modules include related functions including Transportation, Release, Bail, Inmate Schedules, Inmate Jobs, Grievances and Requests, Use of Force, and PREA.

ATIMS offers Add-on License Capabilities to the base product at an additional cost, which may be installed as part of the current implementation, at the County's option, including:

1. ATIMS / Fulcrum Biometrics – Fingerprint identification and registration at Intake, Release, and Kiosks for inmates , and can be used as personnel fingerprint recognition when logging into the JMS. 3rd Party Fulcrum product ATIMS manages as OEM. 10 Fulcrum biometric readers are included.
2. Embedded Dynamic Imaging (DISI) Mugshot Camera - Mugshot Photo is taken using DISI software and controlled camera, embedded into ATIMS software. The camera capabilities are integrated with inmate intake and booking functionality and can be used for SMTs as well. This license includes 1 mugshot camera and associated hardware. Additional camera kits would be at additional cost.
3. ATIMS Mobile – Provides JMS functionality on mobile devices used by the correctional staff in native iOS and Android, and provides hardware integration to cameras, barcode, QR readers, and other devices. Hardware is not included.
4. ATIMS Identification Scan – Provides functionality with a driver's license scanner used by correctional staff for intake and visitor-related tasks.
5. ATIMS Inmate Self-Service Functionality – Provides secure booking, visitation, appointments, incident, and grievance information and allows inmates to place requests and receive responses. This requires integration with other correction vendor systems – commissary, inmate phone, etc. Hardware is not included.
6. ATIMS Who's in Custody Website – An external website that allows the public to search for specified data about the current inmate population.
7. RFID Technology Integration – Integration with the Agency's preferred RFID Inmate Tracking System. Hardware is not included.

Technical Architecture & Requirements

ATIMS' software is a browser-based system operating on a Microsoft Windows environment with the MS-SQL database. It is designed and developed as Single-Page Application with Angular and ASP.NET Core. As a browser-based system, it operates on the client's web browser with the software running on a Windows IIS server.

ATIMS will implement their JMS Software-as-a-Service (SaaS) platform to be accessed by the Sheriff's Office staff through the County's approved internet browsers on County-issued computers and mobile device. ATIMS will provide single sign-on (SSO) functionality via Active Directory integration as specified by the County.

The JMS application will be compliant with FBI CJIS Security Policy 5.9.4 and future policies, including the requirement to provide multi-factor authentication for users to access CJIS information. ATIMS will notify the County immediately if any compliance issues are found.

The County may require ATIMS to provide clustering and replication functionality.

Technical Environments

ATIMS will provide the following environments to the County:

- Production (including Disaster Recovery/Failover)
- Test
- Training
- Development

ATIMS shall provide, configure, manage, and support each environment as specified in this SOW. The environments will include all third-party software required for their operation and ATIMS will automate the migration of configuration and administrative settings (including user accounts and roles) between and across the environments. Environments advisable or needed for data conversion staging or testing are not included in the above list.

The Test, Training, and Implementation environments will hold all of the County data. At least one environment will mirror Production.

System Requirements

- During implementation and post Go-Live, the County environments will be maintained pursuant to the ATIMS hosting terms and specifications (See Exhibit L: Support Agreement)
- The environments will be deployed with an initial ATIMS provided base configuration.

During the project, interim ATIMS JMS platform releases will be tested by ATIMS to ensure that they meet performance and functional requirements and have no adverse impact on the County's configuration.

New software releases will first be deployed to Implementation or Test, as specified by the County, followed, on County's approval, to the remaining environments within [1] day of approval.

The project will be implemented using the latest version of the JMS, which is currently at Version 2.6. ATIMS will make available all future Updates and releases which, upon County approval, will be deployed to County environments by ATIMS.

Services

Implementing the jail management system requires detailed and extensive planning and guidance from ATIMS. Included in the Agreement's fee schedule are professional services as noted throughout this Statement of Work, including:

1. Implementation of the software purchased.
2. Configuration and customization (Enhancement) of the software to include Highly Critical, Critical, Highly Desirable and Desirable functional requirements not currently supported by the JMS or included on the JMS roadmap. These configurations and customizations are listed in the ATIMS proposal and in Exhibit D: Requirement Fees where a Configuration, Enhancement, or a Form is provided for a fee.
3. Travel, upon prior written approval by the County, of specified personnel to County onsite locations, for the implementation, and support of the jail management system project.
4. Hosting, and Application Management Services of the County's JMS in multiple environments, through implementation and post release. [See Exhibit K: Support Agreement)
5. Warranty, Maintenance, and Support Services, following Go Live . [See Exhibit K: Support Agreement)

The Professional Services, referenced above, include:

.

1. Project Management	SOW: Section D, Phase 1 Inception
2. Implementation	SOW: Section D, Phase 1 Inception
3. Business Analysis	SOW Section E, Phase 2 Elaboration
4. Application Configuration	SOW Section F, Phase 3 Build
5. Design & Development	SOW Section F. Phase 3 Build
6. Interfaces and Technical Staff Training	SOW Section F, Phase 3 Build
7. Data Conversion	SOW Section F, Phase 3 Build
8. Forms and Reports	SOW Section F, Phase 3 Build
9. Testing	SOW Section F, Phase 3 Build
10. End User Training & Documentation	SOW Section G, Phase 4 Transition
11. Go Live	SOW Section G, Phase 4 Transition
12. Post Go Live	SOW Section G, Phase 4 Transition

Each of the above services will be provided during one or more project phases and includes related deliverables which are noted in their respective sections in the SOW.

Requirements

The County Requirements consisting of Functional requirements, Non-Functional (Technical) requirements and Interfaces for this project are included in the below exhibits with ATIMS responses and clarifications on how ATIMS and their JMS Software will meet County requirements.

Requirements
Exhibit M - Non-Functional (Technical) Requirements
Exhibit N - Functional Requirements
Exhibit O - Interfaces

Period of Performance - Project Start and Timeline

Project Start

Upon execution of the Agreement, the ATIMS team will immediately initiate the project and start preparation and mobilization of its resources in accordance with the requirements defined in the Statement of Work.

Project Timeline

The implementation time period, from Project Kickoff to Go Live (production use of the JMS after the final data conversion), is estimated to take between 18 and 24 months. A 90-day Post Go Live Stability Period is required before Final Acceptance by the County of the JMS (See Section C Acceptance Process - Final Acceptance).

Following Go Live, post Go Live deliverables may be scheduled for delivery as agreed to by the County and delivery of these items may overlap the Stability Period. The SOW Testing and Acceptance process will govern delivery and acceptance of any Post Go Live deliverables. Final Payment under the Payment and Fee Schedule will not be invoiced until County acceptance of all Post Go Live deliverables is issued.

Project Schedule

As part of the Planning Phase, the ATIMS and County Project Managers, in consultation with ATIMS and the County, will develop a Project Work Plan (Schedule) [Deliverable 5] which will be used as the project baseline. The Kickoff date (project start) will be jointly agreed to and based on the availability of ATIMS and County resources. The Project Work Plan, as with all Deliverables, will require County approval.

Project Structure

Implementation Phases

This project will be implemented in multiple phases, with each phase including distinct tracks, activities, deliverables, milestones, and acceptance by the County.

At a high level, the project implementation approach includes four phases: Inception, Elaboration, Construction and Transition.

Phase 1: Inception

Main Activities: Kick off the project, conduct initial discovery, create and finalize the Project Management Plan (including subplans) and the Project Plan and Schedule, and install the base JMS in the hosted environment.

The Planning Track (1) of the Inception Phase establishes the framework of activities and mechanisms by which to manage the project. The Project Management and implementation teams are assigned, roles and responsibilities are identified, and initial planning actions are taken for the project Kickoff including preparing the agenda and discussion materials.

- During the Installation Track (2), the latest version of the base JMS is installed in required hosted environments, documentation is provided, and initial training of the core County project team occurs.
- Annual Recurring fees including SaaS Hosting are not accrued or incurred by County until completion of the project and post go-live.

Phase 2: Elaboration

Main Activities: Analyze the current legacy JMS system and County business practices, validate the SOW requirements against County expectations and JMS functionality, conduct a Gap Analysis incorporating As Is and To Be analysis.

The Elaboration Phase includes the Business Analysis Track (3). ATIMS will perform business analysis Requirement validation and a Gap Analysis.

Phase 3: Build

Main Activities: Perform build activities including system configuration, development of system modifications, interfaces, data migration, report/forms, and testing of that work.

The Build phase is the longest phase of the project and is when most of the development work is completed. Tracks include Configuration (4), Modifications (5A), Interfaces (5B), Data Migration (5C), Forms and Reports (5D), and Testing (6). The ATIMS testing team will perform required testing tasks during Track 6 as well as test enhancements, interfaces, and the data migration as that work is provided in each of their related tracks, updating the RTM concurrently.

Phase 4: Transition

Main Activities: Train the Trainers, Train the end users, perform final data migration, execute Go Live, complete post Go Live activities, close the project.

Tracks during this final phase include Training (7), Go Live (8) Post Go Live (9) and Close (10). The Training track includes Administrative, Technical, and Train the Trainer training conducted by ATIMS, and End User Training, conducted by the County with assistance from ATIMS. During the Go Live track, the Go Live date is confirmed, pre-Go Live activities, including the final data conversion occur, and production use of the JMS commences.

Phase Activities

Each phase will include one or more tracks (sub phases). Each track may include a milestone which will be composed of one or more deliverables, and each deliverable will be composed of multiple tasks. Individual tasks will be assigned to ATIMS, the County, or be a joint responsibility. Certain tasks can be performed

concurrently and may overlap multiple tracks which will require attention to ensure resources are not overallocated.

Deliverables

A Deliverable is a distinct work product or element that can be individually examined for completeness, accuracy, quality, and acceptance. Examples of deliverables include project documentation, meetings, plans, reports, software modifications, integrations, and other defined work. Certain deliverables, as defined in this SOW, are considered living documents or ongoing processes (e.g., Project Management Plan, Requirements Traceability Matrix, Documentation, Testing) and will be updated throughout the implementation as warranted.

Certain specified deliverables may require a Deliverable Expectation Document (DED) that will further define the delivery process, expectations, requirements, ATIMS and County roles and responsibilities, and acceptance criteria.

Deliverables will be reviewed by the County PM, Business and Technical Leads, and subject matter experts to ensure that deliverables produced for the County conform to SOW and DED requirements and meet County quality standards. The County will accept deliverables or identify deficiencies that require remediation.

Activities
An activity or task is a work element that may be a stand-alone requirement or necessary for completion of a Deliverable but is not itself subject to acceptance.

Milestones
A milestone represents the completion of an activity that must occur in a project time cycle for a particular Track to meet the project objectives. Milestones mark the completion of incremental steps or parts of work generally comprised of project deliverables. A Milestone may be tied to a specific payment. (See Exhibit X: Payment and Fee Schedule)

The Acceptance process and criteria for Deliverables is described in Section C: Acceptance Process)

Stage Gates

Stage Gates are used to assist in monitoring the progress of the project and schedule compliance. Stage Gates are used to signify the completion of a set of work and may coincide with completion of one of the four project phases or completion of a track within a Phase.

Stage Gates for this project are:

1. Planning
2. Requirements / Design
3. Configure / Build
4. User Acceptance
5. Cutover

The Acceptance process and criteria for Stage Gates is described at p. 48-49.

Post Implementation

At the conclusion of the Transition Phase, upon Final Acceptance, the ATIMS Support team will take over from the Implementation team and ATIMS will provide warranty, support (post Go Live maintenance), and hosting services as provided by the Agreement.

Work Breakdown Structure (WBS)

A Work Breakdown Structure is a hierarchical breakdown of the project with each descending level representing a more detailed view of the project work (e.g., phases, tracks, deliverables, tasks, and activities). At a high level, the project is categorized by phases. Each phase is broken down into tracks, with each track containing work packages. A work package may itself be a deliverable or include multiple deliverables as well as multiple tasks and activities.

Deliverables by Phase

Following is a list of Deliverables by Phase and Track:

Phase	Track	Deliverables
Phase 1: INCEPTION		
	1) Planning	1. Kickoff Presentation 2. Kickoff 3. Discovery & Walkthrough 4. Project Management Plan (PMP) 5. Project Work Plan (Schedule) 6. Project Management Artifacts 7. Requirements Traceability Matrix (RTM)
	2) Installation	8. Base JMS - Installation 9. Base JMS - Documentation 10. Core Team Training
Phase 2: ELABORATION		
	3A) Business Analysis	11. Business (Gap) Analysis 12. GAD – Draft Gap Analysis Document (GAD) 13. GAD – Review Workshop 14. GAD – Final Gap Analysis Document (GAD)
	3B) Analysis - Modifications	15. Modification – Design Specifications
	3C) Analysis - Interfaces	16. Interfaces – Interface Plan
	3D) Analysis - Migration	17. Conversion Planning Workshop(s) 18. Conversion Plan 19. Data Map

Phase 3: BUILD		
	4) Configuration	20. Configuration – User Roles & Security 21. Configuration – System Administration 22. Configuration – Modules (with Workflow)
	5A) Build – Modifications	23. Modifications - Development (Test Fixes)
	5B) Interfaces	24. Interfaces - Interface Control Documents (ICD) 25. Interfaces – Development & Testing
	5C) Migration	26. Test Runs (ETL) 27. Final Conversion Report
	5D) Forms & Reports	28. Forms – Specifications 29. Forms – Development & Testing 30. Reports – Specifications

Phase	**Track**	**Deliverables**
		31. Reports – Development & Testing
	6) Test	32. Acceptance Test Plan (ATP) 33. Performance Testing 34. System Testing 35. User Acceptance Testing (UAT) 36. Final Test Report
Phase 4: TRANSITION		
	7) Train	37. Training Plan 38. Training Documentation & Materials 39. Forms – Training 40. Reports - Training 41. Admin & Technical Training 42. Train the Trainer (T3) Training 43. End User Training (EUT) 44. Final Training Report
	8) Go Live	45. Go Live Plan 46. Go Live Preparation 47. Conversion Cutover 48. Go Live – On Site Support 49. Transition to Support
	9) Post Go Live	50. Post Go Live Deliverables 51. Post Implementation Evaluation Report (PIER)
	10) Close	52. Project Close Out

B) ROLES & RESPONSIBILITIES

County and ATIMS Joint Responsibilities

Joint responsibilities include:

- Assign well-qualified dedicated Project Managers with authority to direct and coordinate work to lead their project teams.
- Provide Subject matter experts (SMEs) who have experience and authority in their areas of expertise and are designated the primary contact in their relevant area. SMEs include technical representatives responsible for data conversion and migration, data interfaces, testing, and training as well as functional domain representatives who can provide guidance regarding business operations and expected use and configuration of the software.
- Establish a clear executive oversight and escalation path, including an Executive Committee of key County and ATIMS executive representatives to provide oversight to the project team and monitor project progress. The Executive Committee is separate from any internal customer decision-making authority (e.g., a County Project Steering Committee). The County and ATIMS Project Managers will report to the Executive Committee.
- If either party is aware or becomes aware of a delay that will prevent ATIMS from meeting a scheduled deliverable or milestone, such party will promptly inform the other party of such delay, and the reason, in writing. Similarly, County activities which are or may be delayed that will affect an ATIMS deliverable will also be promptly reported. The Project Managers will confer and determine remedial actions and possible changes to the schedule, escalating the matter as appropriate.

ATIMS Responsibilities

ATIMS is the sole contractor for this project and, as such, will provide guidance, consultation, and technical expertise required to accomplish the project goals, and will provide all of the Vendor deliverables cited herein, unless otherwise agreed to by the County in writing.

ATIMS responsibilities, in addition to those specifically listed elsewhere in this SOW, include:

Administrative Requirements

- Provide single point of contact account manager who will serve throughout the term of the Agreement
- Provide an implementation project manager and implementation services support personnel
- Understand and comply with SCC Policies and Procedures throughout the Implementation
- Execute the approved Project Management Plan and overall implementation methodology
- Ensure appropriate and required personnel attend all required meetings and sessions

- Ensure project continuity in the absence of any given team member
- Ensure timely replacement with qualified resources upon the removal or loss of an ATIMS project team member
- Maintain appropriately qualified, security cleared personnel throughout the engagement, notifying the County Project Manager in a timely manner if personnel changes are required
- Comply with all information and data security standards for all SCC information and documentation in ATIMS control as per agreed upon with County and in compliance with the FBI CJIS Security Policy and the CLETS PPPs.
- Implement and maintain version control on all documentation, plans, etc. delivered between parties throughout the relationship
- Record all remote workshop and training sessions
- Record meeting, workshop, and demonstration decisions and action items
- Update the Requirements Traceability Matrix as needed

Services Requirements

As may be further defined in the respective sections of this SOW, ATIMS shall be responsible for:

- Project Management of ATIMS Team efforts
- Software installation and Initial Setup
- Configuration including refinement based on County use
- Software requirements gathering and reporting
- Software design specification and development
- Training and development assistance with ATIMS supplied report-writing tools
- Interfaces – Analysis, design, development of all interfaces between the JMS and ISE or any approved point to point interfaces with a third-party system.
- Data Migration – Analysis, design, and development of data migration efforts.
- Correction of defects throughout implementation
- Training Plan and curriculum development
- Training, including Administrator, Technical, and Train the Trainer
- Testing and Technical support, including during User Acceptance Testing (UAT)
- Technical and functional (application) knowledge transfer throughout the implementation
- Post-implementation support
- Professional and technical services as outlined in the SOW

Project Management

The ATIMS Project Management Team shall plan the activities to be carried out in the project, the assignment of resources to those activities, the dependencies among those activities, and their timing. The ATIMS PM Team shall establish a project control and reporting system, using a combination of MS Project and JIRA, to

provide routine and realistic assessments of the project progress through the completion of the project against approved milestones and detailed plans.

Working with the County JMS Project Manager, the ATIMS Team Project Manager shall establish roles, responsibilities, record-keeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.

The ATIMS Team Project Manager shall provide the County with ongoing project management including weekly status reports, status meetings, and project work plan updates. The ATIMS PM Team shall prepare a baseline risk management plan and update the plan regularly (at a minimum, monthly) over the course of the project, or more frequently, if needed.

ATIMS Resources

Qualifications

ATIMS is required to provide a project team that is timely, engaged, responsive, and communicates effectively, including, unless the County agrees to a lower utilization rate during specific time periods, a full-time dedicated Project Manager throughout the implementation. Resources shall have a deep working knowledge of, and experience with, the ATIMS JMS, multiple JMS implementations, environments similar to the County in size and complexity, a broad understanding of criminal justice, business processes described in this SOW, and be fully capable of performing their duties as assigned. County must approve all ATIMS project staff members.

Subcontractors

ATIMS may supplement ATIMS staffing resources with additional partner resources to be selected from ATIMS's certified and approved partners without any additional charge to the County. Any subcontractors will be identified in the Staffing Plan and will be managed in the same manner as other ATIMS resources. As with ATIMS staff, the County retains the right to review, vet, and accept/reject subcontractor resources. County also reserves the right to request the removal of any subcontractor resource in the same manner it would request the removal of an ATIMS Resource. Subcontractor resources will be paid by ATIMS and will be part of the Fixed Price arrangement unless County has agreed to a valid Change Request through the Change Management process.

County requires that ATIMS disclose the fact that a resource is a subcontractor along with the nature of the subcontractor's relationship with ATIMS prior to assignment. ATIMS shall be solely responsible for all work performed by any subcontractor.

Scheduling of subcontractors will occur per the project plan as a particular skillset is required and ATIMS is unable to provide qualified resources. At such time, the ATIMS Project Manager and the County Project Manager will coordinate and schedule the respective subcontractor and direct them to begin their work.

Removal

The County reserves the right to dismiss a ATIMS project team member if he or she no longer meets the expectations of the County.

If an ATIMS team member is removed, ATIMS shall provide an acceptable resource replacement and assign him or her to the project in the same capacity as the previously removed resource. The new resource shall be added to the project as soon as practical or as otherwise agreed upon by the parties.

Maintaining a vendor qualified and operational project team is a SOW requirement. Excessive turnover of ATIMS resources, in the sole judgement of the County, will trigger a review of the project by the County and ATIMS executive management to review causes, remediation, and mitigation of future turnover.

Responsibilities

The table below describes the primary roles, and the high-level responsibilities of ATIMS resources. Additional roles may be added as the project progresses. In some cases, more than one role may be filled by the same person. As well, some roles may require more than one resource at various times.

ATIMS Role	Responsibilities
Project Sponsor Felix Rabinovich Vice President, ATIMS	• Partner and collaborate closely with the County Project Sponsor • Provide high-level oversight of the ATIMS project team, performance, and adherence to contract requirements • Resolve issues and risks escalated by the Project Managers or the County Project Sponsor • Support staffing commitments and requirements for the project • Assist in removing execution obstacles

Project Manager	• Manage and coordinate resources staff in conjunction with the Technical Manager in compliance with the Statement of Work and Project Plan. • Collaborate closely with County Project Manager • Communicate on a regular basis with the County's Project Manager to address issues and ensure that project tasks are being completed in a timely manner • Create, maintain, and distribute, in coordination with the County Project Manager, Project Plans and related monitoring and management tools. • Chair regularly scheduled review and status sessions • Attend project events, meetings, and workshops, preferably onsite • Create and distribute status reports • Track and update project Action items, Issues and Risks, including mitigation strategies, and manage them through resolution • Respond to County requests for assistance and clarification • Help the County understand any issues that may have an impact on the project plan and timeline of milestone deliverables • Direct all questions to the County Project Manager regarding the configuration of the software and any other questions arising under the terms of the contract, relying on the instructions and information received from the County Project Manager • Plan, schedule, coordinate and track the implementation with County • Ensure that tasks are completed on schedule • Identify and mitigate issues and risks, and escalate as needed in a timely manner • Enforce project governance and structure in regard to change control, communication, and escalation management • Maintain project portal
Technical Architect/Lead	• Primary technical liaison

ATIMS Role	**Responsibilities**

	• Provides oversight of JMS Contractor Technical resources and recommendations • Leads the design and development of software including JMS modules & functions, forms, reports, dashboards, interfaces, etc. • Provides guidance regarding application functionality and implementation strategies • Resolves technical issues with County architect and support resources • Translates analysis models into designs and executable software
Configuration Release Manager	• Responsible for Management and Control of all software components specific to the project • Prepares and validates all installation processes and procedures • Participates in and supports the onsite installation of the configured system • Prepares all software release packages and patches • Maintains all environments throughout the life cycle of the project
Implementation Consultants	• Lead/participate in configuration analysis • Develop report specifications • Develop business automation/validation specifications • Aid in UAT issue resolution • Support Go-Live activities • Provide support to the Technical Consultant • Provide support to the Training Consultant • Manage and assist in the development of Business Rules specifications • Manage and assist in Unit Testing • Manage Business Rules deployment
Conversion Manager	• Oversees all aspects of the data conversion activity • Works closely with the ATIMS' PM to ensure data migration is on track • Works with the Project Team to address and mitigate any data migration risks and issues • Works with the Test Manager to troubleshoot and resolve testing issues • Prepares the data conversion Plan for the project • Reviews data conversion approach and deliverable expectations

ATIMS Role	Responsibilities
	• Oversees data mapping and ETL design specifications • Executes and supports data conversion for testing and go-live • Develops and unit tests integration and data migration components (ETL) according to design • Supports production cutover activities
Conversion Developers	• Manage data migration analysis and interface requirements • Prepares data mapping and ETL design specifications • Prepares interface design specifications • Participates in design reviews with other team members • Develops and unit tests integration and data migration components (ETL) according to design • Participates in code reviews with other team members • Supports end-to-end integration testing, mock conversion testing and user acceptance testing • Troubleshoots and resolves testing issues as required • Supports production cutover activities • Transitions to knowledge to support team
Report Lead	• Manage and assist in the development of report specifications • Manage and assist in the development of reports • Manage and assist in Unit Testing reports • Manage report deployment
Interface Manager	• Oversees all aspects of the interface development and integration • Prepares the interface integration plan • Oversees creation of interface design specifications • Responsible for all resourcing of the interface development activity • Works closely with the Project Manager to ensure interface development and integration is on track • Works with the project team to address and mitigate any interface risks and issues
Interface Developer(s)	• Conduct Interface analysis sessions • Develop data integration specifications for importing or exporting data from the JMS System • Unit Test data integration programs
Testing Manager	• Oversees all test Team tasks • Prepares Test Plan and ensures it is followed throughout the Project life cycle

ATIMS Role	Responsibilities
	• Coordinates with the product Development Team to ensure critical issues are addressed • Responsible to ensure adequate test resource assignments • Supports end-to-end integration testing, conversion testing and user acceptance testing
Training Manager	• Leads all training activities • Design training curriculum and schedule in accordance with County needs and business processes • Delivers JMS Training classes • Collaborates with the Organizational Change Management Lead • Prepares Training Plan for County project training activities
Trainers	• Conducts Train-the-Trainer training sessions • Tailors Workflow™ product training materials for project • Works closely with County trainers • Collaborates with the Organizational Change Management Lead

County Responsibilities

The list below describes the County's responsibilities, in addition to those specifically listed elsewhere in this SOW, during the implementation of this Project.

- Arrange the logistics of all the onsite meetings
- Provide the County Business Calendar with County holidays and black out days, including out of office days for key project staff
- Ensure County attendees are invited in advance and are present for all applicable meetings
- Provide adequate facilities and equipment for Training
- Review and provide feedback on all deliverables within the timeframe specified in the respective Deliverable Expectation Document or SOW, as applicable
- Provide adequate facilities for ATIMS team members when onsite
- Provide adequate departmental resources to support the project timeline while taking into consideration daily and periodic departmental work requirements
- Provide appropriate data, information, and cooperation necessary for the data migration and creation of any data exchanges (interfaces)

County Resources

The table below lists the primary roles for the County and the high-level responsibilities of each. Additional

County roles may be added as the project progresses. The County may determine that in certain situations, more than one County role can be filled by the same person and roles may, at various times, require more than one resource.

County Role	Responsibilities
Project Sponsor	• Partner and collaborate closely with the ATIMS ty Project Sponsor • Have ultimate authority and responsibility for the project • Provide high-level oversight throughout the duration of the project • Act as vocal and visible Project champion • Approve major project deliverables • Approve schedule, budget, quality and/or scope change requests • Assist in removing execution obstacles • Create an environment that promotes teamwork and user adoption • Ensure project aligns with County strategy and goals • Facilitate cross-project and cross-functional collaboration (when needed to meet objectives) • Garner support from all County stakeholders • Prioritize project to demonstrate importance • Support the Project Manager's administration, collaboration, and cooperation efforts • Collaborate with the PM to resolve escalated issues and risks • Secure additional funds for budget changes
Business Lead	• Has joint responsibility, along with the Project Sponsor, for the success of the project • Work with Project Sponsor to implement policy, procedure and/or department changes to support the new solution • Responsible for partnering with the Project Manager to enable project success • Allocate operational resources as needed to support the success of the project • Assist Project Manager in reviewing project deliverables and artifacts. • Create and maintain business requirements in close partnership with the Business Analyst

County Role	Responsibilities
	• Create and maintain the business process flow diagram(s) in close partnership with the Business Analyst • Responsible for identifying any policy, procedure and/or department impact • Responsible for on-time delivery of business tasks in close partnership with the Business Analyst • Work closely with Business Analyst to plan and complete User Acceptance Testing (UAT) • Work closely with Business Analyst to plan and deliver training to the business stakeholders • Work collaboratively with Core Project Team to complete project deliverables • Works with ITP&A and PM to approve vendor invoices
Project Manager	In consultation with the County: • The Project Manager will act as the single point of contact for project related communications and have the authority to make project related decisions, in consultation with County. • Allocate County resources, including staff, external interface vendors, information, • Establish project priorities • Hold internal meetings as necessary with County staff to discuss work, expectations, risks, and constraints related to project scope, schedule, budget, and quality • Ensure County attendees are present for all applicable meetings, workshops, discussions, and conference calls as necessary. • Collaborate closely with ATIMS Project Manager • Maintain regular communications with the ATIMS Project Manager and Project Team • Assist the ATIMS Project Manager in development of project documents and secure internal approval and signoffs • In coordination with the ATIMS Project Manager, develop strategies to mitigate risks and issues, taking corrective actions as necessary. • Facilitate objectives of project meetings in conjunction with the ATIMS Project Manager • Create and administer the Project Communication Plan with the ATIMS Project Manager and any change managers. • Create and maintain the Project Schedule with the ATIMS Project Manager

County Role	Responsibilities
	• Create and maintain the Risk Register • Create and maintain the Project Management Plan with the Project Sponsor, Core Project Team, and the ATIMS Project Manager. • Plan, schedule, coordinate and track the implementation with the ATIMS Project Manager and across departments within the County • Review status reports and provide feedback and actions as necessary • Centralize reporting and severity assignment of issues into ATIMS online issue-tracking system • Administer Project Change Control to govern schedule, budget, quality, and scope changes • Bring the need for policy changes to the attention of the Business Lead SME • Identify and mitigate issues and risks, and escalate as needed in a timely manner • Drive and facilitate collaboration with Project Sponsor and Core Project Team to complete the Project Charter • Work with team members to complete tasks by providing reasonable target dates and follow-up • Work with the Core Project Team to develop and execute adequate training • Work with the team to develop and execute adequate testing • Enforce project governance and structure in regard to change control, communication, and escalation management • Escalate unresolved decisions, tasks, or interpersonal issues to Project Sponsor and/or PMO management • Lead the team in partnership with vendor project team members • Monitor vendor contract compliance
Business Analyst	• Assist in the creation of the Operational Plan • Create and execute a test log to track testing and defect resolution • Create and maintain the business process flow diagram(s) in close partnership with the Business Lead SME

County Role	Responsibilities
	• Create and maintain the business requirements in close partnership with the Business Lead SME • Create test plan • Ensure appropriate level of detail in test scripts (depends on who is testing) • Ensure completeness of test scripts for each module, interface, and data conversion • Prepare test results for UAT approval • Prepare training session rosters for all training sessions • Primary owner of business requirements activities and mapping of requirements to any vendor-provided software • Provide input to Communications Plan for testing • Provide input to OCM and Communications Plans for Training • Responsible for easing the understanding of how technical solutions will solve business requirements • Responsible for planning and delivering training to the business stakeholders in close partnership with the Business Lead SME: • Responsible for planning and leading the completion of UAT in close partnership with the Business Lead SME • Review vendor training materials to ensure depth and coverage is adequate • Validate training materials readiness for end user training • Validates that software has been configured to support business requirements and business processes • Work with PM to coordinate training session schedules and logistics • Work with PM to determine testing logistics and create testing schedule
Subject Matter Experts (SME)	• Assist in the creation of to-be analysis documents, specifications for reports, automation, interfaces & conversions • Attend product training • Fully engaged in the business analysis and system configuration activities

County Role	Responsibilities
	• Gather data as necessary for the project and make decisions about business processes • Participate in test planning, test script development and user acceptance testing • Review and test the system configuration • Works with the Change Manager to execute proposed business changes.
Technical Leads **Technical Product Owner,** **Sr. Engineer**	• Oversees all County technical responsibilities • Act as the primary technical resource • Primary point of contact for County legacy systems • Develops custom software including forms, reports, queries, dashboards, interfaces, etc. • Manage integration and interfaces with other systems and serves as primary point of contact for all County interfaces • Provides guidance regarding application functionality and implementation strategies • Work with ATIMS technical resources during implementation
Technical Resources **(Network, Integrations and Conversions)**	• Attend product training • Understand the reporting, interface and data conversion needs of County • Build or modify reports, interfaces, and data conversion scripts as needed
Change Manager	• Primary contact for all Change Management throughout the project • Responsible for change management planning and execution • Works with County and ATIMS Project Managers to schedule activities related to change management • Participates in all functional activities to assess related impacts on the business • Works closely with the ATIMS Training Manager
Change Agents	• Collaborates with the County Change Manager • Mentors new users on the new JMS and processes • Champions the new JMS • Supports all training activities
Testing Lead	• Manages end to end functional testing, integration testing, and data migration testing.

County Role	Responsibilities
	• Primary point of contact for all County testing activities.
Testers	• Develops and executes test cases with County SME's • Records test results during testing activities and logs issues as required • Updates test cases as required • Maintains defect log as required
Training Lead	• Participates in the development of the project Training Plan • Manages all County training activities • Primary point of contact for Training • Schedules all training sessions, including attendees and facilities • Plans, schedules, and coordinates County training
Trainers	• Participates in specified training • Customizes County training materials

Key Resource Availability & Substitution

The key ATIMS personnel listed below are essential to the work being performed under this SOW. Key personnel will remain on the project and dedicated to their assigned tasks as long as they remain in the employ of ATIMS or a substitute with substantially similar skills, background and experience is promptly provided by ATIMS, with the approval of the County, as described below.

Key Personnel:

- Project Sponsor: Felix Rabinovich
- PMO Oversight
- SME Oversight Michael Haberkorn
- Project Manager
- Technical Lead

If a project team member identified as key personnel terminates employment with ATIMS or takes a leave of absence, ATIMS shall submit to the County fifteen (15) working days in advance of staff departure from the project a written request for replacement of such personnel with substantially similar skills, background, and experience. The request must include justification, propose replacement staff, a detailed resume, and provide sufficient detail to permit County evaluation of the impact on the project. Staff proposed as replacements must meet or exceed the education, experience, and other technical requirements of the key personnel being replaced and shall not have any cost impact to the County.

The County will communicate a decision on the proposed replacement to ATIMS in writing within ten (10) working days after receipt of all required information. No change in key personnel or assignment of ATIMS personnel to the project shall be made by ATIMS without the prior consent of the County. In urgent situations where the required advance notice is not possible a verbal request by ATIMS to replace key personnel may be approved by the County. Within five (5) working days of this approval, ATIMS will submit the written request and justification. The County will communicate a decision on the replacement to ATIMS in writing within ten (10) working days of receipt of all required information.

In the event resources proposed as replacements for key personnel do not meet or exceed the education, experience, and other technical requirements of key personnel being replaced, the County reserves the right to require that alternative replacement resources be provided.

C) ACCEPTANCE PROCESS

Deliverables

Overview

Notice and Acceptance
ATIMS will provide formal notice to the County of the submission of a project Deliverable in the form of a Deliverable Notice, and completion of a Milestone in the form of a Milestone Notification.

Acceptance Criteria
Acceptance Criteria is defined in the SOW or in a Deliverable Expectation Document (DED), which will provide additional clarification and description of the deliverable that goes beyond the limited text in the SOW.

Where a Deliverable has a related DED:

- ATIMS will meet with the County PM to refine the acceptance criteria for each deliverable beyond what is included in the SOW.
- ATIMS will subsequently develop a DED for each deliverable.
- The County Project Manager will provide input within seven (7) Business Days of receipt, unless mutually agreed upon by the parties
- ATIMS will modify the DED within five (5) Business Days of receipt
- ATIMS and the County will work cooperatively to reach agreement on the DED.

Process Changes
If the deliverable acceptances process as outlined in the SOW requires adjustment, ATIMS and the County

Project Managers will discuss any such change in advance to reach mutual agreement and will communicate the proposed change to the appropriate stakeholders from both parties, seeking their input where necessary. A mutually agreed-to change to a DED, requirement, Stage Gate, or the acceptance process, with no impact to cost, scope, or Go Live date will not require a change request but will be documented in the Project Management Plan and the Work Breakdown Structure.

Project Deliverable Acceptance Process

Deliverables are classified as either Software or Project. Non-Software items such as documents (e.g., The Project Management Plan) or meetings (e.g., Kickoff) are Project deliverables and will be accepted according to the following process.

1. ATIMS will deliver all Project Deliverables accompanied by a Deliverable Notice by the delivery date as established in the Project Plan. If ATIMS is unable to meet the delivery date, ATIMS shall provide written notice, including a new proposed delivery date, as soon as possible but not less than two (2) weeks prior to the delivery date for meetings and one (1) week for artifacts or activities.
2. Unless otherwise noted, County will review the Project Deliverable within seven (7) Business Days {"Acceptance Review Period") of receipt of the Project Deliverable and provide Acceptance, reject the Deliverable, notifying ATIMS of the reason(s) for non-Acceptance, or request additional time for review.
3. If the County has rejected the Deliverable, ATIMS must, within three (3) Business Days, respond in writing addressing the points raised by County and resubmit the deliverable within five (5) business date from the original delivery date or agree with the County on a new delivery date.
4. County will, within three (3) Business Days of receiving ATIMS written response issue a reply. If the Deliverable has not yet been resubmitted or a new delivery date agreed to, ATIMS and the County will set a new delivery date and the County will review the Deliverable per this process or as otherwise agreed to.
5. ATIMS and the County will repeat the above process until a Deliverable defect is remediated and the County signs off on the Document Deliverable. Either party may escalate the acceptance issue if they believe the delay is unreasonable or are unable to come to terms on the delivery process and related dates.
6. If payment is tied to the Deliverable, ATIMS will not issue an invoice until the Deliverable has been Formally Accepted.
7. For a specific deliverable, the acceptance process may be overridden by a specific DED or previously accepted relevant deliverable terms (e.g., Test Plan, Conversion Plan, Training Plan) and may also be waived by the County Project Manager or modified by mutual agreement of the Project Managers.

Software Deliverable Acceptance Process

In addition to internal testing by ATIMS before release to the County, software is subject to County Acceptance at the end of the following processes:

- Unit/Functional Testing
- Interface Testing

- Data Migration Testing
- System Testing
- Performance Testing
- User Acceptance Testing (UAT)
- Final Acceptance Testing (FAT)

In this context, Software includes:

- JMS modules and functions as configured to meet County requirements
- Modifications, including enhancements
- Interfaces
- Data migration
- Workflows and Wizards
- Reports, Forms, and Dashboards

This acceptance process shall govern County acceptance of all software unless noted otherwise by a DED, or in the UAT (See p. 125) or FAT (See p. 147) sections of the SOW. Notice of delivery is required for each Deliverable and each Software based Deliverable will progress through the established test phases in accordance with the Test Plan and DEDs.

1. A Software-based Deliverable will enter a Test Phase only if the entry criteria for the applicable Test Phase, as set out in the Test Plan or DED, have been met or if otherwise agreed by both parties in writing, and/or as further defined in the Test Plan.
2. All reported defects will be triaged and categorized in accordance with the defect severity and definition table (See p. 46) .
3. County will issue a Notice of Acceptance within ten (10) Business Days of receipt of the Test Summary Report from ATIMS (unless otherwise noted or mutually agreed upon by the parties), if it is determined that:
    - All Test Cases within the applicable Test Plan have been executed successfully and signed off by County
    - ATIMS has fixed and retested all Severity Level 1 (Critical), Severity Level 2 (High), and Severity Level 3 (Moderate) Defects.
    - ATIMS has fixed and retested all Severity Level 4 (Low) Defects, or the County has agreed that any Level 4 Defects may be deferred per an agreed timeline.
4. ATIMS will use its best efforts to install all patches intended to remediate identified defects in sequential order. Once patches are installed, the County will test the patch and confirm it/they resolve the reported defect(s) as soon as practicable, generally within ten (10) days of delivery.

5. Resolution of one defect may introduce new defects. Those new defects are considered unique and will be managed according to their unique presentation, consistent with the Acceptance Process
6. A Software-based Deliverable may only exit a Test Process if ATIMS has demonstrated to the County in a Test Summary Report that the exit criteria for the Test Phase, as set out in the Test Plan or DED have been met, County has verified the exit criteria, and County has signed off on the Test Summary Report by issuing a Notice of Acceptance.

Defect Resolution

ATIMS will utilize ticketing software (e.g., JIRA) to track County reported issues with JMS software functionality or performance. During testing, each County tester will have their own account to log and track reported issues. The County PM and key County staff (e.g., Project Sponsor, Business Lead) will have global access to all tickets.

The County shall submit a report of a JMS functional or performance issue as an "Error". Upon confirmation and acceptance of the Error submission by ATIMS, the Error will be considered a "Defect" and the responsibility of ATIMS to resolve.

ATIMS will install software patches to fix and resolve Defects at no additional cost to the County. Once fix patches are installed, the County will test the fix and confirm if it resolves the reported Defect(s) within ten (10 days of delivery. Defects must be affirmatively closed by the County. Defects are not considered closed or accepted by the passage of time or nonresponse.

Failure to Pass Process

1. If ATIMS has completed a Test but has not satisfied the established acceptance criteria, ATIMS, in consultation with the County, will determine the reason for the failure and the parties will agree on a new test date upon which date a further test will be carried out on the same terms as the initial test, or as otherwise agreed by the parties. Prior to the date for the further Test, ATIMS will use best efforts to remedy all failures specified in the notice.
2. If, after the additional test has been carried out, County determines that the Software-based Deliverable does not fully satisfy the acceptance criteria, County will notify ATIMS of this in writing.
3. Upon receipt of a notice as indicated above, ATIMS will use best efforts to remedy the failure specified in the notice within an agreed period, at which time a third round of Tests will be conducted.
4. If the defect is not resolved after the third round of tests, the parties will agree on a subsequent testing schedule. If after a mutually agreed upon number of additional testing rounds or time period, all failures have not been addressed in accordance with the established acceptance criteria, the Software-based Deliverable in question will be escalated via the agreed upon Escalation Plan in the SOW for resolution, including further testing, modification of the requirements or testing criteria, adjustment of fees, or other actions.

Rejection by ATIMS

In limited circumstances, ATIMS may reject a County-reported Error as not constituting a Defect. All Errors rejected by ATIMS must be in writing and for one of the following reasons:

1. The Error requires a change to the intended design that is clearly outside the scope of the JMS documentation and specifications or the SOW and Deliverable requirements.
2. The Error is not a software Defect but is a training, configuration, setup, or other non-code base software matter. In this situation ATIMS will inform the County as to the reason for the Issue, detail and/or demonstrate the corrective action to take and provide assistance as necessary to allow the County to resolve.
3. ATIMS cannot reproduce the Error. If ATIMS believes they need additional information to understand or reproduce the Error, the County will provide requested information and/or ATIMS and the County will review the Error together to facilitate understanding of the issue. If ATIMS is unable to replicate the Error, ATIMS and the County will work together to attempt to replicate the Error. An inability to replicate the Error on ATIMS test or developer environments is not a reason to reject the Error if it continues on County environments.

Notwithstanding the above, a software Error reported by the County will be considered a Defect if the software:

1. Does not function in accordance with SOW requirements or project deliverable specifications
2. Does not confirm to JMS documentation, specifications, or ATIMS representations.

Should ATIMS reject an Error, ATIMS will provide a detailed explanation in writing of the rejection. ATIMS and the County will meet to review the error and the rejection explanation, including demonstration of the Error and reference to requirement documentation as necessary. If after review ATIMS continues to reject the Error and the County does not accept the ATIMS rejection, ATIMS and the County will escalate the Error and the Error will be reviewed and negotiated at the business level, according to the escalation path.

Defect Severity and Definition

For purposes of reporting and resolving errors during the project, ATIMS and the County will use the same severity level categorization and definition as provided in the Support Agreement.

PRIORITY and Severity Levels	CRITICAL - 1	HIGH 2	MODERATE - 3	LOW - 4
Description	• System down • Critical issues with, or inability to perform core functions or critical processes of JMS • Security breaches and other security issues • Business risk is Critical.	• Software Application Program errors without application workarounds • Incorrect calculation errors impacting records • Severe performance issues impacting critical processes • Business risk is High	• System errors that have workarounds • Performance issues not impacting critical processes • Usability issues • Reporting Issues • Business risk is moderate	• Report formatting • Aesthetic issues • Recommendations for enhancements on system changes • Low to minimal impact
Response Time	< 30 minutes	1 hour	2 hours	8 hours
Update Frequency	Every 30 min	Every 2 hours	Every 24 hours	Every 10 business days
Resolution Goal	Within 30 minutes.	Within 2 hours.	Within 5 business days	Within 30 business days. Placed in queue and resolved in order of importance

Escalation Path

In the event the Project Managers are unable to reach resolution on any issue arising under this SOW, including Defects and the performance of the SaaS environment, the issue will be escalated by the Project Managers.

The following table represents the escalation levels and representatives for ATIMS and the County:

Level	ATIMS Representative	Client Representative
3	Felix Rabinovich, Vice-President	
2		

1		

Stage Gates

A Stage Gate is used to determine that key deliverables and work is complete at specific points in the project before authorization is given by the County to proceed to the next phase or track. A Stage Gate may coincide with completion of one of the four project phases or completion of a track within a Phase.

The Quality Stage Gate process requires ATIMS and the County to:

1. Agree upon activities and deliverables to meet each of the five (5) Quality Stage Gates.
2. Perform the activities to complete the agreed upon Quality Stage Gate deliverables.
3. Present deliverables in Quality Stage Gate walkthrough/review.
4. Obtain County sign-off on agreed-upon Quality Stage Gate deliverables.
5. Obtain County approval to begin execution of activities to meet the next Quality Stage Gate

Stage Gate Acceptance Criteria

Following are the default acceptance criteria for each of the Stage Gates which may be modified by the County.

Quality Stage Gate 1 - Planning

Quality Stage Gate 1 will be complete, when the following has occurred:

- Project Scope has been defined in the approved Project Management Plan
- Planning Deliverables and Schedule has been approved
- Project Governance has been established
- Project Team has been established and onboarded
- Project Kick-off Presentation has occurred
- Environments have been established (dev, test, training, pre-prod)
- Baseline software deployed

Quality Stage Gate 2 – Requirements Design

Quality Stage Gate 2 will be complete, when the following has occurred:

- Gap Analysis has been completed and approved, recommended options have been reviewed and selected, decisions have been logged in the project Decision Log
- Requirements Traceability Matrix has been updated based on the outcome of the Gap Analysis.
- Design Specifications for Modifications (Enhancements, Configurations, and other agreed to work) are complete
- The Interface Plan is complete
- The Data Migration Plan and Initial Data Map are complete.
- Architectural Review Board (ARB) Technical Design Review (TDR) has been completed and approved by

the County

Quality Stage Gate 3 – Configuration/ Build

Quality Stage Gate 3 will be complete, when the following has occurred:

- Software configuration is complete
- Modification (Enhancements & Configuration) development is complete
- Interface and data exchange development complete
- Migration Test Runs are complete.
- Required Forms and Reports are developed and successfully tested.

Quality Stage Gate 4 – Testing & User Acceptance

Quality Stage Gate 4 will be complete, when the following has occurred:

- Functional, system, and regression testing is successfully completed
- Performance testing is successfully completed
- UAT scripts developed and tested by County
- All identified Severity Level 1 & 2 Defects are resolved
- Final Test Report is complete

Quality Stage Gate 5 - Cutover

Quality Stage Gate 5 will be complete, when the following has occurred:

- Train the Trainer Completed
- Technical Training Completed
- End Users have been trained per the Training Plan
- Final Documentation completed and provided to County
- Only cosmetic and low priority defects remain
- Go-Live readiness assessment complete
- Go-live support resources in place
- Production environment ready, including user credentials
- Final data conversion ready for execution
- Operational Readiness Review (ORR) completed and approved by the County

Final Acceptance

County's use of the JMS and/or any Services during the implementation or production use of the system shall not constitute Final Acceptance.

Final Acceptance ("Acceptance") will not occur until the JMS has completed a 90-day Post Go Live Stability Period - performing for 90 consecutive days in a live production environment without Severity Level 1 or Severity Level 2 errors, and satisfactory resolution of Severity 3 and 4 Errors. If a Severity Level 1 or 2 Error is reported and confirmed as a Defect, the 90-day period will be reset to provide a 90 consecutive day period

without error unless explicitly waived by the County in writing.

ATIMS will provide a System Final Acceptance document. This document shall include a final RTM that identifies and confirms the completion of all SOW requirements

The System Final Acceptance document will be submitted upon the successful completion of the 90-day Post-Go Live stability period.

While the Warranty and Support period will begin upon Go Live, sign off on the System Final Acceptance document by the County Project Manager is required to constitute Final Acceptance by the County.

D) PHASE 1: INCEPTION

TRACK 1) Planning

The Inception Phase includes the Project Planning Track (1) and Installation Track (2) of the base JMS, with related documentation and training of the Core Team to use the system.

Project Management Methodology

The County will provide overall project management. The ATIMS Project Manager will manage ATIMS resources and services in consultation with the County Project Manager.

The ATIMS Project Management process is critical to ensure the JMS implementation is completed on time, on budget, and meets project goals. This project uses a hybrid methodology with a modified waterfall implementation approach augmented by agile development of system Modifications, Interfaces, and the Data Migration.

The Project Planning Track of the Inception Phase provides an opportunity to ensure the project starts in a well-organized, structured fashion while re-confirming the County and ATIMS expectations regarding the implementation.

Process Overview

During project initiation the ATIMS Project Manager will create the project management planning deliverables in consultation with the County Project Manager, including the Project Management Plan and the Project Work Plan (Schedule). These documents provide the structure for ongoing management and tracking of the project in accordance with the agreed approach, methodology, tools, and standards.

ATIMS will follow project management implementation processes and methods consistent with:

1. Project controlling documents including the SOW and DED requirements
2. County standards and guidelines
3. ATIMS experience in best practices when implementing their JMS for customers similar in size and

complexity

4. The Project Management Institute (PMI) Standards and Guidelines

ATIMS will plan the activities to be carried out in the project, the assignment of resources to those activities, the dependencies among those activities, and their timing. ATIMS shall set up internal roles and responsibilities and project record-keeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.

ATIMS shall establish a project control and reporting system to provide routine and realistic assessments of the project progress through the completion of the project against approved deliverables and milestones.

The County will Identify and assign qualified resources to the project including functional and technical Subject Matter Experts (SMEs), testers, and trainers.

Key Activities:

In coordination with the County, ATIMS will perform the following project management activities throughout the implementation across all Phases and Tracks:

1. Development and Management of a Project Management Plan (PMP)
2. Project Document and Versioning Management
3. Resource Management (ATIMS Staffing)
4. Schedule Management
5. Communications Management (Status Reporting/Stakeholder Communications)
6. Quality Assurance, including Quality Gate Reviews
7. Risk and Issue Management and Escalation
8. Scope and Requirements Management, including Requirements Traceability
9. Cost Management
10. Change Request Management
11. Performance Management (Project and System)

Project Management Tools

While the County and ATIMS may maintain their own project management tools for internal tracking, reporting, and resolving issues, collaboration between ATIMS and the County is necessary to ensure an efficient implementation and project success.

To ensure ATIMS and the County maintain effective communication and transparency, multiple project management tools will be utilized. These tools will be maintained by ATIMS with the County having access and edit ability.

Key project management tools that will be used to help manage this project include:

Project Management Plan (PMP)
The Project Management Plan is the master plan controlling the project. It describes the project methodology, scope, reporting structure, timelines, assumptions, and risks. The PMP contains multiple related subplans, including Communication Plan, Risk Management Plan, Training Plan, etc. The PMP is a living document and will be reviewed and updated as appropriate, at least quarterly, throughout the project by ATIMS.

Project Work Plan (PWP) (Project Schedule)
Often thought of and referred to as the "Schedule," the Project Work Plan will be maintained by ATIMS in Microsoft Project (MPP). The Work Plan tracks project phases, tracks, tasks, deliverables, and milestones as well as the schedule and resource allocation for tasks.

Actions, Agreements, Issues, and Risks (AAIR) Register
The AAIR Register (equivalent to a RAID Register), is an integrated MS Excel tool that will track project artifacts, including Action items, Agreements (decisions), Issues, and Risks. The Issues Log and Risk Register are subsumed within the AAIR Register. Owners, status, and related dates will be tracked and updated at least weekly by ATIMS.

Requirements Traceability Matrix (RTM)
The RTM is a modified version of the County's RFP Technical (RFP Appendix A) and Functional (RFP Appendix B) Requirement documents, including the ATIMS response to those documents. All requirements, including new and modified requirements, are tracked in the RTM which will also track related information, including linkage to functions/screens/reports, where the requirement can be found, test results, and delivery/acceptance dates. Management and updating the RTM is the responsibility of ATIMS.

Project Status Reports (PSR)
Project status will be tracked, managed, and reported by ATIMS on an ongoing basis. A status report provides a complete, holistic view of the project at a point in time. ATIMS will provide written weekly (or as agreed to by the County) Project Status Reports. A PSR includes a review of project health, budget, schedule, current activities, upcoming activities (the next 60 days), issues, and risks.

Status Meetings
ATIMS will lead weekly (or as agreed to by the County) status meetings to review the PSR and discuss project related topics. Attendees will include the Project Managers, key ATIMS and County team leads, and others as appropriate.

Project Manager Checkpoint Meetings
Regularly scheduled meetings between the ATIMS and County PMs will be held as needed, but no less than weekly (or as agreed to by the County), to review and assess the project's status, progress, issues, risks, current and planned mitigation actions and next steps.

Quarterly Project Reviews (QBR)
Project Reviews (meeting and written report) will be conducted at least quarterly to review status, assess performance (included what has, has not worked), review current and upcoming action items, evaluate risks and issues, and "look ahead" to major deliverables in the coming 90- and 180-day period. QBRs will include the ATIMS and County Executive sponsors and other executive management as considered appropriate by the County.

Change Register
The Change Register will track all change requests and related information, including relevant dates (e.g., date submitted, date approved), type of change, a description of the change, decision, and cost (if any).

Document Management Repository
The County and ATIMS will collaborate on a document and information repository (e.g., SharePoint) to track and manage project documentation. The County will have full access to all project documents.

Issue Tracking Software
ATIMS will provide Sonoma County with access to their issue tracking software (Jira or similar tool). The County Core team will have access to all project tickets.

Communication

Overview
Project Communication is key to a successful project. The County expects communication to be complete, clear, and timely. The Communication Plan, to be developed as part of the Project Management Plan, will provide details on communication types, methods, frequency, and related information. It is incumbent on all parties to raise issues and concerns as soon as known.

All direct communication between ATIMS and County personnel will be copied to the Project Managers and staff as agreed by the PMs. Email shall be considered appropriate written communication.

Project communication between the County and ATIMS teams will include recurring weekly project status reports and meetings to ensure all aspects of the project are discussed and remain on track.

Scheduling of the status meetings, agenda and meeting minutes delivery, action item tracking and escalation will be defined and agreed to between the County and ATIMS project managers during the Initiation and Planning Track.

Schedules and appropriate escalation trees will be communicated to all responsible stakeholders. The primary points of contact will be the project managers for ATIMS and the County.

Black-Out Date Calendar
To support the efficient and timely scheduling and completion of tasks, The Project Managers will maintain a master calendar of key resource availability.

At the beginning of the project and each calendar year, and as otherwise appropriate, the Project Managers will agree upon the holidays that will be observed for both organizations and adjust the schedule accordingly. On an ongoing basis, Project Team members will also provide planned days out of office, including personal time off. There may be other identified dates and scheduling conflicts which may be considered in the same manner and should be noted (user group meetings, training, professional conferences, etc.).

Change Management

Overview

In a project of this size and complexity, it is expected that changes will be made to tasks and timelines during the course of the implementation. Many of these changes are likely to have minor impact on the project as a whole and can be agreed to and memorialized by the Project Managers. Examples include but are not limited to, DED details, acceptance criteria, schedule changes that do not affect the Go Live date, removal or modification of deliverable requirements, and certain process changes.

Significant changes to project scope, budget, or schedule, however, must be governed by the change control process which is required to:

1. Assess and document the impact of scope changes on project schedules, resources, prices, payment schedule, deliverables, acceptance criteria, and other provisions affected by the proposed change.
2. Provide a formal vehicle for approval to proceed with any SOW material changes.
3. Provide a project audit record of all material changes.

This is a fixed fee engagement with fixed requirements, fixed deliverables, and an agreed upon project schedule and methodology. Absent major changes to requirements or roles and responsibilities of ATIMS, change orders for additional funding for the JMS Implementation are not anticipated by the County. Delays caused by ATIMS or by the failure of ATIMS to achieve signoff using the agreed signoff process will not be cause for change orders.

Change order requests for additional funding will only be submitted/considered under the following circumstances:

1. County initiates substantial changes or additions to the functional requirements that constitute a material departure from the requirements set forth in the RFP, and such changes or additions will require substantial additional work. The County and ATIMS shall jointly determine the materiality of such changes or additions and whether they are outside the scope of this SOW.
2. County requests changes to deliverables that are materially different from what is described in this SOW or agreed upon through the Deliverable Expectations Document (DED) process defined in the agreement.
3. Work of a substantial nature that the SOW indicates is to be performed by County or County Third Parties (e.g., integration partners) is shifted to ATIMS during the course of the project.

If a change is identified that meets the above criteria, the County and ATIMS Project Managers will invoke the Change Management process. The process will determine any impact to the project budget and, as appropriate, a Change Request will be created for review and approval by ATIMS and the County.

Change Control Process

Any changes (modifications, additions, and deletions), to the work process and effort described in the SOW will be memorialized in writing between the Project Managers.

In the case where the County or ATIMS determine a change is required, the requesting party will complete a Change Request (CR) form and advance the CR for review and sign off by the other party. The status of the Change Request and its approval are monitored by the project managers. The project schedule, cost, and resources are updated as needed.

Upon approval and execution by each party, a CR will become a Change Order and form part of this SOW. If the Parties do not execute and deliver to one another a Change Order, the prior obligations of each party under this SOW will remain unchanged.

All Change Orders will be signed by authorized representatives of ATIMS and the County and, if a Change Order requires additional funds, extension of the Agreement term or other reasons determined by the County such Change Order will be incorporated into the SOW by written amendment to the Agreement signed by both parties, prior to commencing any activities defined in the Change Order.

All changes are recorded on the Change Log [SEE Track 1 Planning]. A sample Change Request is provided in Attachment [4]

Change Request Initiation

In addition to process, activity or deliverable changes, the Change Management process may begin whenever a project team member identifies a significant issue with the JMS meeting an existing or new County requirement, or a requirement is no longer needed. The project team will meet to discuss ATIMS and County expectations and options to meet the requirement. If ATIMS believes the County has misunderstood or is unaware of how the JMS functions, ATIMS will provide additional information on system functionality and/or may conduct a "show and tell" session to demonstrate functionality or a system workaround.

If the County continues to believe a change is necessary, it will initiate a Change Request and the process will be managed by the project managers.

Should project team members identify a feature gap, the ATIMS project manager will perform an analysis to determine whether the gap is a product defect or is a new or additional feature request needed to address missing required functionality.

New Feature Request

If the issue is a new feature request:

1. The ATIMS Project Manager creates an internal enhancement tracking ticket, shares the tracking number with the County, and includes the information in the RTM, if applicable.
2. The enhancement ticket is assigned to the ATIMS Product Director, who determines whether the feature and/or functionality should be added to the development road map.
3. Roadmap (No additional fee) If the Product Director decides that the new feature will be included in the ATIMS roadmap as a future product feature:
    a) The defect ticket is assigned to the Product Director, who prioritizes the item for product development.
    b) The defect fix is scheduled for a future release.
    c) When completed, the fix is released to the project team, who will test on an internal client

environment that includes configuration of other enhancements, if applicable.

4. Change Order (fee based) If the Product Director decides that the new feature should not be included as a product feature, the Product Director notifies the ATIMS Project Manager of this decision.
   a) The ATIMS Project Manager creates a Rough Order of Magnitude (ROM) estimate for the new feature and sends the ROM to the County Project Manager.
   b) The County discusses the ROM internally, may review the previous discussion regarding workarounds, and then decides how to proceed.
   c) If the County decides to proceed with the enhancement, the requirements change management process ends and the project-level change management process begins. This process is documented in the Change Management plan which is in the Project Management Plan (PMP).

Approval

Change Requests that result in a Change Order, must be approved by the County Project Sponsor, ATIMS Project Executive and Project Managers (County and ATIMS).

The parties will jointly determine whether a proposed Change Order requires a separate statement of work (e.g., a new product) or if it will be incorporated into this statement of work.

All Change Orders will be signed by ATIMS and the County and, if determined necessary by the County, incorporated into the Agreement by written amendment signed by both parties, prior to commencing any activities defined in the Change Order.

Fee Tracking

Any County approved addition, modification, or removal of fees (e.g., through a change order) will be tracked in the AAIR Register and via an update to Exhibit B: Payment and Fee Schedule.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

1) Kickoff Presentation	**Type: Document** **DED: No**
Description	To prepare for the Kickoff, the ATIMS PM will create a Kickoff Presentation, using MS PowerPoint or a similar tool, and including related documents and information to be distributed to and discussed by attendees at the Kickoff meetings.

Requirements	The Kickoff presentation will, at a minimum, include: 1. Project Overview 2. ATIMS & County Implementation Team 3. Objectives and Definitions 4. Implementation Process, Phases and Tracks 5. Project Schedule 6. Artifacts 7. Roles and Responsibilities 8. Keys to Success 9. Next Steps 10. Questions and Answers (Q&A)
ATIMS Activities	Create the Kickoff Presentation Submit the Kickoff Presentation to the County PM for review and acceptance. Incorporate County feedback into the Kickoff Presentation
County Activities	1. Ensure participation in the project planning activities as this will be a pre-requisite to the development of the kick-off presentation
Acceptance Criteria	1. Presentation materials conform to the SOW, agreed upon topic agenda, and reasonable business standards.

2) Kickoff	Type: Meeting DED: YES
Description	The Project Kickoff is a minimum three (3) day event and consists of a series of meetings (conferences described in detail below) and presentations that sets the expectations of the participants and ensures all project stakeholders have an agreed upon understanding of the project scope, implementation process, objectives and schedule while addressing any outstanding issues, concerns and/or questions. The objective of the Kickoff is to communicate the objectives of the project, gain commitment from the team and explain the roles and responsibilities of each stakeholder. From the County, in attendance should be the Project Manager, technical staff with major responsibilities (e.g., installation, data migration), Sheriff's Office representatives, Executive Management, and other key stakeholders. From ATIMS, in attendance will be the ATIMS Project Sponsor, Project Manager, ATIMS Technical Lead, ATIMS Business Analyst, and others as appropriate. During the kickoff process, ATIMS and the County will review and discuss key administrative topics, including, but not limited to: 1. Project Objectives and Goals 2. Stakeholders 3. Expectations 4. Project Scope 5. Project Methodology and approach 6. Project Schedule 7. Resource Needs 8. Roles & Responsibilities 9. Communication Framework 10. Project performance measures and critical success factors (Keys to Success)

Requirements	**<u>Project Conference:</u>** The purpose of the Project Conference is to review and ensure agreement on: 1. County and ATIMS Expectations The SOW, including roles, responsibilities, deliverables, and milestones Status reporting requirements and format 2. Procedures governing acceptance of deliverables, milestones, and invoices. 3. The draft Project Management Plan (prepared by ATIMS) 4. The draft Project Work Plan (Schedule) (prepared by ATIMS) 5. Project Artifacts 6. Change Control Procedures 7. Testing Process and Procedures, 8. Roles and Responsibilities **<u>Technical Conference</u>** The purpose of the Technical Conference is for ATIMS and the County to review technical considerations and possible issues that relate to the implementation of the JMS. Topics to include: 1. ATIMS JMS hosted environments including technical requirements, performance standards, and system administration User Account and Role based security management System backup and disaster recovery Environment and System security Desktop and network requirements Configuration System modification design and development process Data migration Interfaces **<u>Executive Sponsor Session and Kickoff</u>** The purpose of the Executive Session is to present a high-level review of the Project implementation process, contract, schedule and a short walkthrough of the software to County executives and stakeholders. Key to this presentation is the need for stakeholder approval, communication, involvement, and a focus on the keys to success.

	<u>System Presentation and Kickoff</u> The purpose of the System Presentation and Kickoff is to provide a forum for the SO to engage their staff, raise awareness and buy-in for the project. The System Presentation and Kickoff may be conducted in place of or in addition to the Executive Session and Kickoff depending on the needs and preferences of the County. Audience members can include the core Project Team, Executives, and SO management and line staff.
Joint Activities	1. Schedule mutually agreeable date(s) to conduct the Kickoff 2. ATIMS Program Management, County leadership, and key County staff co-present on the objectives, values, expectations of the project 3. Conduct the Project Conference 4. Conduct the Technical Conference 5. Conduct the Executive Session 6. Conduct the System Presentation and Kickoff
ATIMS Activities	1. Prepare agenda and meeting materials for all meetings including PowerPoint presentations and handouts. 2. Track and follow-up on action items, including questions and concerns.
County Activities	1. Provide meeting room facilities and equipment to accommodate the Kickoff 2. Arrange attendance for necessary attendees 3. Prepare for Executive leadership and key Project staff to co-present on the objectives, values, expectations of the project and the importance to the County.
Acceptance Criteria	1. Completion of Kickoff meetings and conferences and achievement of meeting goals.

3) Discovery and Walkthrough	Type: Activity DED: No
Description	A Discovery process and walkthrough of the jail facilities allows ATIMS staff to better understand SO procedures and business operations in more detail than provided in the original RFP. ATIMS and the County will conduct a high-level review of SO business practices and workflow to establish a familiarity of the SO environment. At the same time, since it will have been several months since County personnel may have last viewed the application, ATIMS staff will conduct overviews of the software and its capabilities.
Requirements	1. ATIMS and County will agree on the scope of Discovery activities 2. ATIMS and County Project Managers and appropriate project leads and subject matter experts will be in attendance.
ATIMS Activities	1. Conduct high-level review of SO operations 2. Conduct walkthrough of jail facility 3. Conduct JMS application overview
County Activities	1. Secure permissions and clearances to allow ATIMS staff to enter County facilities and jail. 2. Arrange attendance of necessary managers and SMEs.
Acceptance Criteria	1. Completion of the Discovery and Walkthrough

4) Project Management Plan (PMP)	Type: Document DED: YES
Description	The PMP will identify milestones, project deliverables, staffing assignments, tasks, payment schedules, change order procedures, risk analysis, respective responsibilities and establish monitoring and control procedures.

Requirements	**PROJECT MANAGEMENT PLAN** Develop the PMP as defined in the SOW and DED. The PMP shall include, at a minimum, the following sections and subplans: 1. Project Management 2. Project Organization 3. Roles and Responsibilities 4. Stakeholder Identification and Engagement 5. Project Deliverables & Receivables 6. Customer Furnished Equipment 7. Hardware/Software Acquisition Inventory 8. Supplier/Subcontractor Management 9. Project Communication (Ongoing/Regular and Event Based) 10. Security and Proprietary/Protected Data Considerations 11. Risks and Issues Management 12. Knowledge Management 13. Business Continuity Plan 14. Cutover, Acceptance Criteria, and Stage Gates 15. Monitoring and Incident Management Plan 16. Qualifications 17. Technical Approach 18. Implementation Methodology 19. Technical Plan and Documentation 20. Change Management The PMP will be modified based on requirements, considerations and clarifications identified in the Project Conference and updated through the implementation.

SUB PLANS

The PMP is composed of related supporting (sub) plans, including at a minimum:

Quality Management Plan

The Quality Management Plan provides the processes, methods, and tools to be used by ATIMS and the County to ensure the proper management of the project and that a sufficient level of quality of the deliverables is maintained throughout the life of the project. Quality measures and techniques are specific to the type of deliverables being produced and will be specified in the Deliverable Expectations Document for project deliverables. The Quality Management Plan will include the following elements.

1. Defined quality assurance responsibilities.
2. Detailed definition of all deliverables by phase and associated acceptance criteria.
3. Project deliverable review and acceptance process.
4. Regularly scheduled reviews of key project phases, stage gate exit criteria and milestones.

Communication Plan

The Communication plan provides the processes, tools, and methods that will be used to ensure effective communication of information among stakeholders and the project teams, including cadence and artifacts for both the JMS team and external stakeholders. The Communication Management Plan includes:

1. Types of meetings and frequency including, status meetings, stakeholder meetings, project scrum meetings
2. Communication methods (email, reports, presentations, etc.)
3. Cadence
4. Distribution methods
5. Approach for documenting and distributing meeting minutes
6. Collaboration tools

Risk Management Plan

The Risk Management Plan shall establish the framework for identifying, managing and controlling risks, including mitigation actions. It shall also include definitions and processes to identify concepts of risk, impact and probability.

	The object of Risk Management is to exploit or enhance positive risks (opportunities) while avoiding or mitigating negative risks (threats). Based on the plan, ATIMS shall document and communicate known risks and evaluate potential risks in all phases of the implementation. The Risk Management Plan will be used to: 1. Create and update the Risk Log (Risk Register). 2. Anticipate and identify risks. 3. Identify the severity and quantify the potential impact of each identified risk. 4. Quantify the probability of each identified risk. 5. Support the development of risk mitigation plans for each identified risk. 6. Provide guidance for assessing the efficacy of risk mitigation actions. 7. Describe work products and processes for assessing and managing risks. 8. Detail the escalation and remediation mechanisms for risks. 9. Detail how risks and issues will be tracked and reported and the format of risk and issues reports (depth, detail and content). **Change Management Plan** The Change Management Plan covers both technical and non-technical changes. The Change Management Plan will be used on an ongoing basis to do the following: 1. Manage the Change Request process. 2. Analyze the impact of Change Requests. The impact of the proposed Change Request will be documented in the Change Request Form. 3. Track the authorization or denial of the Change Request. The authorization or denial will be in writing using the Change Request Form. 4. Track the status and completion of any Change Orders (authorized Change Requests). **Stakeholder Management Plan**

	The Stakeholder Management Plan provides a structured approach to the identification and engagement of all stakeholders. The Stakeholder Management Plan includes: 1. Identification of all project Stakeholders (both internal and external and expectations and level of interest/support/influence in the project 2. Stakeholder register (position, location, contact details) 3. Engagement plan for each stakeholder (communication / engagement strategy)
Joint Activities	1. All Plans are jointly developed by ATIMS and the County and require County approval.
ATIMS Activities	1. Provide a draft PMP, including subplans, based on the SOW and DED and work with the County PM to develop a final PMP to be provided 2 weeks after the Kickoff. 2. Facilitate and lead discussions to finalize the various subplans within the PMP. 3. Incorporate related decisions made during the project planning and kickoff meetings into the PMP. 4. Maintain the PMP on an on-going basis throughout the life of the project and update it, in collaboration with the County's PM as necessary, but no less than quarterly.
County Activities	1. Review and provide input and written comments on the Project Plan and Supporting Plans 2. Approve the project plan 3. Approve each of the supporting plans
Acceptance Criteria	1. The PMP, including any sub or related plans, meets the acceptance criteria as defined in the SOW and DED, with resolution of any County concerns.

5) Project Work Plan (Schedule)	Type: Document DED: YES
Description	The Project Work Plan is a Microsoft Project document that provides a Project Schedule including Work Breakdown Structure, Resource Allocation, Gantt charts and a project calendar. The Work Breakdown Structure (WBS) will define the project's overall objectives by describing the project phases, tracks, tasks, deliverables, and milestones.
Requirements	The Project Work Plan will include: 1. A consolidated view of the project tasks and activities including task descriptions 2. Task duration, start and finish dates. 3. Resources (ATIMS and County) assigned to each activity and their required level of effort. 4. Task prerequisites 5. Identification of all deliverables and milestones, with the deliverables clearly linked to the appropriate milestone. 6. A critical path analysis and reporting process.
ATIMS Activities	1. Provide a draft Work Plan, and work with the County PM to develop a final Work Plan to be provided 2 weeks after the Kickoff. 2. Incorporate County feedback into the Project Work Plan 3. Maintain the Project Work Plan on an on-going basis throughout the life of the project and update it, in collaboration with the County's PM as necessary, but no less than weekly to reflect the accurate status of the project. 4. Upon approval by the County, establish the Project Work Plan as the baseline for the schedule for the project.
County Activities	1. Provide necessary County based information including schedule and resource constraints, dependencies, conflicts, and requirements.
Acceptance Criteria	1. The PMP Meets the criteria as defined in the SOW and DED, with resolution of any County concerns.

6) Project Management Artifacts	Type: Document DED: No
Description	Various customary project management tools and artifacts are required to properly manage the project.
Requirements	The following artifacts are living documents and continuously updated throughout the project. **Project Directory Log** ATIMS and the County will create a Directory of project team members: that will be available to all team members. The log will list: 2. Name Title Agency/Department Role Location (address) Phone Mobile Phone Email Availability **Action Log** The Action Log is used to track Project tasks as determined by the Project Managers and/or noted during Project Status and Review meetings. The Action Log will, at a minimum, include: 1. Tracking Identifier Date Action Item Description Owner Status Date Due Date Closed Notes

Agreement/Decision Log

The Agreement/ Decision Log tracks all major project decisions and agreements within and between the ATIMS and County teams. The decision log will include at a minimum:

1. Agreement/ Decision Number
2. Issue
3. Issue Raised By
4. Decision
5. Decision Description
6. Owner (Decision Maker)
7. Decision Date
8. Decision Description
9. Impacts

Issue Log

The Issue Log will, at a minimum include:

1. Issue identifier
2. Date Issue was Identified
3. Description of Issue
4. Categorization of Issue (budget, schedule, staffing, etc.)
5. Severity of the Issue
6. Issue Mitigation Strategy
7. Action Items and Assignment
8. Status of the Issue (Open, Closed)

Risk Log

Project risks are uncertain events or conditions, that if they occur, will impact the project. Risks will be recorded in the Risk Log and are to be discussed during status meetings. The Risk log will, at a minimum include:

1. Risk identifier

Date Risk was Identified
Description of Risk
Categorization of Risk (budget, schedule, staffing, etc.)
Severity of the Risk
Probability of the Risk
Risk Mitigation Strategy
Action Items and Assignment
Status of the Risk (Open, Closed)

Change Request Log

The Change Log tracks all Change Requests (functional, technical, excluding organizational change management) and will, at a minimum, include:

1. Tracking Number

Date of the request
Priority Rating of the request (classified by County PM)
Category of the Request (Technical or Non-Technical)
Scope Determination (In Scope or Out of Scope)
Requestor Information (name, title, department, contact information)
Impact of Requested Change (budget, schedule, staffing, etc.)
Benefit of the Requested Change
Urgency of the Requested Change (e.g., routine, urgent, immediate, critical)
Authorization or Denial of the Change Request
ATIMS Reason(s) for Denial (if denied)
Status of the Change (in work, not started, on hold)
Required Completion Date
Point of Contact for follow-on action(s)
Due date for next action

Status Report

Status reports will be delivered on a mutually agreed day and time covering the end of a weekly, or otherwise agreed to, time period. These documents will be used as a guideline for the discussion to occur in the required weekly, or otherwise agreed to, status meetings. Project Status Reports will be stored and made available in the Project Library.

Status reports will include the following information:

1. Status of work completed against the Project Work Plan

Actual/Projected completion dates compared to the approved baseline key dates.
Accomplishments in the current period

	Objectives and activities for the next 30-day period Action items Issues and Risks Review - Escalated risks, issues (including schedule and budget), and related action items 7. Mitigation plan for all work activities not tracking to the approved scope, schedule, or budget. 8. 90 Day Look Ahead to assess, review, and highlight any matters that could impact project activities and deliverables 90 days out. Key decisions A graphical summary of the Project by phase, track, and major functional areas. Team resource utilization/impacts (County and ATIMS)
ATIMS Activities	1. Maintain all logs and update as necessary, but at least weekly. 2. Provide all logs in a central location (e.g., Project Library or other shared location). 3. Ensure that activities are taking place as detailed in the artifacts. 4. Provide appropriate responses to County requests for information. 5. Address any escalations collaboratively with the County PM 6. Update the Requirements Traceability Matrix and other artifacts as necessary.
County Activities	1. Review Logs on a weekly basis 2. Review the Status Report in advance of the Status Meeting 3. Provide appropriate responses to ATIMS requests for information. 4. Address any escalations collaboratively with the ATIMS PM 5. Provide input and decisions as needed (approve, deny, etc.)
Acceptance Criteria	1. All components of this deliverable are accepted by the County. 2. Project documents meet the requirements as detailed in the SOW and generally accepted project management standards.

7) Requirements Traceability Matrix	Type: Document DED: YES
Description	The RTM is used to track all project functional and technical requirements for each module or functional area throughout the life of the project. Utilizing an RTM ensures that each requirement has been validated, is met by the product (linking to the module, function, screen), has passed testing (by both ATIMS and the County) and has been accepted by the County. The RTM tracks the original functional and technical requirements, modifications of those requirements as agreed to by ATIMS and the County, and new requirements requested and/or added through the change order process.
Requirements	For each requirement, the Requirements Traceability Matrix (RTM) shall include: 1. Reference to the RFP Appendix A1 and B1 requirements 2. The specific JMS component (e.g., screen, report, workflow, data field, etc.) where the requirement is met 3. The related test case where the requirement is tested, test status, result, date passed/approved 4. The training source, method, document or module where instruction is provided for the requirement (if applicable)
ATIMS Activities	1. Create the initial RTM document using the RFP Functional and Technical Requirements 2. Provide updates to the RTM throughout the implementation
County Activities	1. Provide input and review on the RTM throughout the implementation
Acceptance Criteria	1. The RTM is reviewed and accepted by the County as meeting the project needs. The RTM meets the SOW and DED requirements.

TRACK 2: Installation

ATIMS will establish, configure, and provide access to multiple required environments and install the JMS with a base configuration into each environment. As part of the installation process, ATIMS will provide base system documentation and conduct introductory training of the system to the County Core Team.

ATIMS will provide an Environment Coordination Plan, updateable throughout the implementation as necessary that will ensure that changes deployed to the County are executed in a structured and repeatable manner to reduce the risk of failure.

The Environment Coordination Plan will include:

- The process for rolling out the JMS and future builds/updates to the separate environments, including any dependencies on JMS project activities and any external constraints or dependencies
- The process to provide configuration changes/update across the Development, Testing, Training and Production environments
- Ensure that all release and deployment packages (builds) can be tracked, installed, tested, verified, and/or uninstalled or backed out, if appropriate.
- Ensure that the dependencies between data migration, interfaces and core business functions are addressed and covered in the Test and Production environments

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

8) Base JMS - Installation	**Type: Software** **DED: No**
Description	ATIMS will create the required environments to County specifications and install the latest generally available version (2.6 or higher) of the JMS.
Requirements	**Install the JMS in all required JMS Environments,** including: 1. Implementation 2. Test 3. Train 4. Reporting **User Accounts** 1. JMS will provide user log in authentication against Active Directory. 2. User management (password expiration, lockout, "forgot password" functionality, MFA, etc.) will be enforced by Active Directory. 3. User roles and security will be managed by the JMS, or as agreed to by the County.

	Release Deployment Plan 1. Create a Deployment Strategy Plan. 2. Meet with County to confirm strategy and approach. 3. Align the plan with industry best practices. 4. Ensure that each release package consists of a set of related assets and service components that are compatible with each other. 5. Ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the configuration management system. 6. Ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out, if appropriate. 7. Ensure that change is managed during the release and deployment activities. 8. Ensure that the dependencies between data migration, interfaces and core business functions are addressed and covered in the Test, Train and Production environments. 9. Record and manage deviations, risks, issues related to the new or changed service, and take necessary corrective action. 10. Ensure that there is knowledge transfer to enable the customers and users to optimize their use of the service to support their business activities. 11. Ensure that skills and knowledge are transferred to operations and support staff to enable them to effectively and efficiently deliver, support and maintain the service, per required warranties and service levels. 12. Create a disaster recovery plan. 13. Provide and document automated monitoring and incident notification functionality. **Technical Requirements** ATIMS will ensure the JMS and hosted environments meet all County Non-Functional (Technical) Requirements**,** including County security polices, failover, business continuity, and, if required, clustering and replication.
Joint Activities	1. Test JMS access by the County Core Team Users
ATIMS Activities	1. Create required environments

	2. Ensure Active Directory integration 3. Test all environments to ensure they meet ATIMS performance and SOW standards 4. Provide cloud and administrative management tools and demonstrate their use to the County 5. Monitor and validate conformance to CJIS, NIST, CLETS, and related security policies
County Activities	1. Provide to ATIMS a list of Core Team users who will have access to all environments. 2. Create users in Active Directory 3. Review the Deployment Strategy Plan and provide comments
Acceptance Criteria	1. ATIMS has certified in writing setup of all environments, installation of the JMS with a base configuration, and that the JMS, after installation, has been tested and meets ATIMS functional and performance standards and County, CJIS, and related security policies. 2. Verification by County that all environments are accessible by the County Core Team and the JMS performs as specified. 3. ATIMS has provided a Deployment Plan agreeable to the County.

9) Base JMS - Documentation	Type: Document DED: YES
Description	Documentation, to be provided contemporaneously with the installation of the JMS, must comprehensively cover administrative, technical, and functional areas and topics.
Requirements	Required Documentation includes, but is not limited to: 1. JMS Overview 2. Module/Functionality menu outline 3. Manuals for each module and function 4. Video recordings (generally 5-10 minutes) demonstrating system and module specific functionality 5. Database Dictionary, including an Entity Relationship Diagram (ERD) and/or ATIMS will provide to the County the ability to generate an ERD. 6. Master Reports List and Guidebook (including for each report a description, screenshot, business rules detailing query selection criteria, listing of select/filter and sort parameters, and data element list with descriptions of the elements. 7. Environment administrative, DR, and business continuity Runbooks
ATIMS Activities	1. Provide Required documentation
County Activities	1. Review JMS provided documentation. 2. Notify ATIMS of any documentation deficiencies where the documentation does not meet SOW requirements or fails to adequately meet generally acceptable documentation standards 3. County to assist with development of ATIMS business continuity Runbook.
Acceptance Criteria	1. All required documentation is provided and acceptable to the County.

10) Core Team Training	Type: Training DED: No
Description	Introductory training by ATIMS of the County Core Team is necessary to allow the County Project Manager and Core Implementation Team to understand key system operational conventions, navigation, and capabilities. More detailed training will be conducted during Track 4) Configuration, Track 5D) Reports and Forms, Track 7) Training, and as outlined by the SOW.
Requirements	**Functional Training** Provide functional training to ensure the Core Team understands the system sufficiently to assess what gaps may exist. **Technical & System Admin Training** Provide technical and system administration training to ensure the Technical Staff and System Administrators are able to operate the system, including manage user accounts.
Joint Activities	1. ATIMS and County will collaborate on the type and amount of Core Team training required (one to two days)) at the onset of the project.
ATIMS Activities	1. Provide onsite Training to the Core Team
County Activities	2. Arrange attendance of Core Team members, including technical staff as appropriate.
Acceptance Criteria	1. Completion of Core Team Training 2. A rating of satisfactory or better by the Core Team on the adequacy and quality of the Core Training.

E) PHASE 2: ELABORATION

TRACK 3A: Business Analysis

Overview

Identifying and understanding SO business needs is a necessary condition to implementing a successful solution. This includes:

- Validating the RFP Requirements which requires analysis beyond the descriptions provided in the RFP Functional Requirements.
- Identifying disconnects between the RFP Requirements (once they are better understood), JMS functionality, and ATIMS responses on whether or not they meet the requirements (and how).
- Identifying and reconciling significant SO needs not identified in the RFP Requirements.

To perform the above validation and identification tasks, ATIMS will conduct a business (Gap) analysis. This analysis is expected to lead to a refinement of requirements, and/or agreements between the Project Managers, including Change Orders, as necessary. Any requirement changes will be recorded in the Requirements Traceability Matrix., maintained by ATIMS, with full access, including edit rights, by the County.

This detailed business analysis, is a continuation of the work begun during the Operations Walkthrough and Project Conference during the Kickoff.

Step 1: Requirements Validation Process (Pre-Implementation Analysis)

Validation is intended to confirm that ATIMS' interpretation of the requirements, RFP response, and the available out-of-the-box functionality meet the intention of the County requirement. Any necessary revisions / enhancements or exceptions will be documented in the Gap Analysis, and/or a refinement of project documents as the project proceeds.

In defining the parameters of the proposed JMS implementation, ATIMS and the County will complete an initial review and analysis of all RFP requirements where one or more of the following is true:

- ATIMS initial response required qualification for On-Prem v. SaaS implementation
- ATIMS initial response was **D** (No – The requirement cannot be met)
- ATIMS initial response was **C** (Customization or Modification – The requirement will be met by making programmatic (software development) changes to existing software or developing new software.)
- Initial response included request for further information by ATIMS or prompted questions for clarification from the County

All information from this review will be incorporated into the Gap Analysis deliverable as part of the Business Analysis track and will be maintained and updated throughout the implementation as new information becomes available and/or changes are required.

Requirement validation includes the following tasks:

1. Review of the RFP Requirements.

2. Review of As-Is business processes documentation provided by the SO.
3. Discussing the requirements and their related module functionality with the appropriate SO business units that are the focus of the ATIMS validation sessions.

To perform the task of validating requirements, ATIMS will use the following techniques:

- Interviewing County project subject matter experts (SMEs) to clarify or to add deeper context and information to the requirements.
- Interviewing third-party interface providers to clarify and understand data exchange requirements.
- "Job shadowing," which involves the ATIMS team working closely with SO staff as they perform their tasks related to the documented requirements.
- Creating use case scenarios during collaborative sessions to better understand the expected usage of the system. These use case scenarios may result in updated workflow diagrams for the SO.
- Providing As Is and To Be (future state) process workflow diagrams
- Reviewing legislation related to sentencing rules.
- Reviewing County policies, regulatory policies, judicially imposed requirements, and consent decrees.
- Reviewing SO operations documentation that may exist such as user manuals, forms, etc.
- Reviewing data definition documentation provided by the County.
- Collaborating with County data migration analysts to further clarify data definition understandings.

When the requirements validation activities have been performed, the ATIMS project team will analyze the information that has been collected. The analysis activity results in the following:

- Identification and resolution of possible conflicting or unnecessary requirements between the various team members or project stakeholders.
- ATIMS project members can determine whether the requirements fall into the category of configuration or customization.
- A streamlined approach to configuration of the JMS to most closely meet business needs.
- Clear, complete, consistent, and unambiguous documentation of requirements.

The output of these efforts will be an updated Requirements Traceability Matrix and related project documents.

Differences or issues between the County's requirements and the ATIMS JMS standard (out of the box) functionality will be analyzed by ATIMS and documented in the Gap Analysis Document. Solutions to requirements, where possible, will be provided through existing system configuration options. When configuration does not provide a suitable solution and a system enhancement is necessary, ATIMS, in cooperation with the County, will document detailed functional requirements specifications and produce

designs to meet the requirement, designs will emphasis the function to be highly configurable. Designs require County approval.

The project team will analyze requirements to determine if they fall into project (client specific functionality, e.g., forms, reports) or product(JMS base system) categories. Additionally, this analysis will determine where in the project plan the requirements will fall or what work activities correspond to particular requirements. Accountability and priority for each requirement will also be determined as part of the analysis. Finally, metrics and acceptance criteria must be determined for all requirements in order to provide a baseline for understanding when a requirement has been fulfilled to an acceptable level.

Step 2: Gap Analysis

ATIMS will conduct a Gap Analysis, using information collected via previously noted validation techniques and workshops with County SMEs, and prepare a Gap Analysis Document (GAD) detailing observations, findings, and recommendations.

ATIMS will:

1. Work collaboratively with the County to understand key business challenges and deliver solutions that optimize business processes enabled by the JMS. Using best practices, ATIMS shall work with SO business process owners and subject matter experts to analyze and document existing As Is business processes and performance, develop future state To Be processes, provide illustrative business flow diagrams, define change management approaches and training, and define metrics by which future state process performance can be measured.
2. Continue the work begun in the Initial Requirements Review by working with the County to validate requirements identified in the initial ATIMS response as:
    - **A** (Yes – The requirement can be met with Existing Functionality out-of-the-box; configuration and customization are not necessary).
    - **T** (Third Party Software – The requirement can be met with a third-party software product provided by Applicant, including any work to incorporate the Third-Party Software to work with the Applicant's software.)
    - **I** (Interface – Refers to building an interface to the applications listed in this list of requirements.)
3. Ensure that all confirmed functional and technical requirements are provided by the JMS and document how such requirements are realized and validated in the Requirements Traceability Matrix (RTM). ATIMS shall update the RTM as the project proceeds.
4. Review and analyze County business processes. As part of the analysis activities, ATIMS shall conduct interactive workshops with County SMEs to determine optimal use of the JMS to achieve County business processes. ATIMS shall use the JMS, wireframes (design mockups), business process flow diagrams, functional prototypes and/or pilots to demonstrate current and proposed JMS functionality to County SMEs where appropriate.
5. ATIMS shall work with the County to identify business process changes and/or changes to system functionality to address gaps between County business processes and the JMS; and to identify

opportunities for optimization of processes facilitated by the system. ATIMS shall document business process flows in the context of the JMS.

6. Review / Identify County reporting requirements. ATIMS shall identify JMS reporting capabilities, both fixed and ad hoc, and map reporting requirements to JMS capabilities.
7. Produce solution design documents for all customizations and work with County SMEs to validate the documented solution meets the requirement(s).

Requirement clarifications, modifications, additions, and removals will be recorded in the Requirements Traceability Matrix (RTM). The project team will follow the established change control process as necessary.

Implementation of future state business process changes is the responsibility of the County.

Ongoing Requirements Review

Evaluation of system requirements is conducted throughout the project lifecycle with the accompanying deliverables considered living documents intended to convey a shared understanding of how the ATIMS JMS meets the requirements of the County. After definition of the expectations for each deliverable document, updates will be regularly provided to track new findings and solutions., including after acceptance of a deliverable due to changing circumstances and needs.

Throughout the project lifecycle, the County PM will ensure all team members are reporting requirement status and raising any issues or concerns with their assigned requirements as appropriate. As the project matures there may be situations in which requirements must change or be altered in some way. The project team will follow the established change control process in order to propose any changes to requirements and receive approval from appropriate entities. Ongoing requirements management also includes receiving approval of all requirements by all vested parties as part of project closure.

Any additional gaps that arise after completion of the Business Analysis track will be treated in the same manner, with an analysis to determine if they can be accepted by the SO, managed with configuration, are on the ATIMS roadmap and will be provided in a future release at no charge, or will be accommodated as an enhancement and at what charge.

Any changes, removals or additional requirements that have been formally approved through the Change Control process will be updated in the project Requirements Traceability Matrix.

Changes can include modifying or removing in scope Interfaces, Configurations (including reports) , Forms, and Enhancements which are provided by ATIMS for an additional fee (See Exhibit B: Payment and Fee Schedule and SOW Appendix D: Requirement Fees). If removed or modified, the ATIMS hours allocated to meet a requirement can be reallocated to other work, during the implementation or post Go Live.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

11) Business Analysis	**Type: Activity** **DED: YES**
Description	The ATIMS business analysis will allow ATIMS to better understand County operational policies and procedures, the County to understand JMS functionality, and both ATIMS and the County to identify and reconcile any major differences between ATIMS JMS functionality and County needs not identified in the SOW and translate this reconciliation to specific technical requirements and/or agreements between the Project Managers. The detailed analysis is a continuation of the work begun during the Operations Walkthrough and Project Conference and is necessary to determine how best ATIMS can be used by the County.
Requirements	1. Identification of areas where functionality is present but may not be adequately usable or deemed difficult to use by County staff shall also be included as part of the analysis. 2. All elements of functionality should be addressed including business operations, interfaces, reports, unique data needs, system security, etc. 3. The resulting Gap Analysis Document (GAD) will address areas of configuration, business process change options, and possible development that may be documented in a Change Order or otherwise agreed to be performed by ATIMS.
Joint Activities	1. Coordinate schedules to facilitate necessary interviews and discussions with County staff.
ATIMS Activities	1. Conduct a Requirements Validation Process as outlined in Step 1: "Requirements Validation Process (Pre-Implementation Analysis)" 2. Conduct a Gap Analysis as outlined in Step 2: "Gap Analysis"
County Activities	1. Provide information requested by ATIMS, including documentation regarding current policies and procedures, screenshots of the current management information system(s), process flow maps and use cases (if available), forms, and reports.

	2. Clarify, at ATIMS request, County policies, procedures, and applicable regulations. 3. Review JMS documentation and become familiar with JMS functionality through repeated operation in advance of Business Process Workshops.
Acceptance Criteria	1. Completion of the Business Analysis per the SOW and DED requirements.

12) GAD – Draft Gap Analysis Document	Type: Document DED: YES
Description	The Draft Gap Analysis Document is a written report documenting the business analysis findings, identifying gaps, issues, and concerns discovered during the process to validate the RFP requirements and determine any gaps or disconnects between the JMS and the County's current system, process, and/or needs.
Requirements	The GAD shall include: 1. As Is analysis accompanied by process work-flow diagrams 2. To Be analysis accompanied by process work-flow diagrams 3. Options and Recommendations The Draft GAD will be used to determine gaps and categorize possible resolution including: 1. Acceptance of the system as is 2. Business process modification by the County 3. Configuration of the system 4. Software modifications to be provided in a future planned release 5. Enhancement of the system at a charge pursuant to the Change Order process
ATIMS Activities	Deliver a GAD with sections, including but not limited to the following topics: 1. Analysis Process Overview 2. Summary of Key Findings 3. Functionality (with subsections for each major module area) 4. Data Collection and Requirements 5. Reports (including templates and statistics) and Forms 6. Workflow, 7. Security Requirements and Policies 8. Interfaces

	9. Other Issues 10. Options and Recommendations (including cost information).
County Activities	1. Attend GAD workshops 2. Provide information requested by ATIMS
Acceptance Criteria	1. Delivery of the completed Draft GAD per the SOW and DED requirements.

13) GAD – Review Workshop	**Type: Meeting** **DED: No**
Description	ATIMS will review the Business Process Analysis findings presented in the Draft Gap Analysis Document (GAD) with the County in a workshop.
Requirements	1. ATIMS and County to meet and review the Draft GAD
Joint Activities	1. Coordinate schedules to set a meeting date to allow the attendance of key ATIMS and County resources.
ATIMS Activities	1. Prepare meeting agenda and materials 2. Lead the GAD Review workshop and present key Draft GAD findings 3. Take meeting minutes
County Activities	1. Review the Draft GAD and any other related documents for clarity and completeness. 2. Submit comments to ATIMS in advance of the Workshop. 3. Ensure appropriate County representatives, including domain experts, attend the Workshop 4. Submit comments to ATIMS after the Workshop.
Acceptance Criteria	1. Completion of the GAD Review Workshop and completion of meeting goals.

14) GAD – Final Gap Analysis Document	Type: Document DED: No
Description	Based on the Draft GAD Review Workshop and agreements reached at and after that meeting, ATIMS will finalize the Draft GAD. The Final GAD will be used to aid in determining configuration requirements as well as the need for any software modifications which will be provided by ATIMS as a general upgrade or as an enhancement at a charge pursuant to the Change Order process.
Requirements	1. The Final GAD to be provided within 7 business days of the GAD Review Workshop.
Joint Activities	1. Modify the Project Plan and Schedule to account for agreed upon changes (e.g., Change Orders) to resolve any gaps.
ATIMS Activities	1. Prepare and deliver the Final GAD
County Activities	1. Review the Final GAD and provide comments to ATIMS 2. Provide written feedback including agreement to modify County business practices or authorization of a Change Order.
Acceptance Criteria	1. Delivery of the completed Final GAD incorporating recommendations and agreements from the GAD Review Workshop 2. Inclusion into the Final GAD new sections A) County comments and B) County Decisions

TRACK 3B: Analysis – Modifications

Overview

ATIMS will perform code modifications and add functionality (forms, reports, functions, business logic, etc.) as noted in the Statement of Work and any other requirements subsequently approved by the Project Managers or authorized by a Change Order after project commencement during Track 5A or as otherwise agreed.

In addition to SOW included requirements that require customization that ATIMS has agreed to provide, the County, through the Gap Analysis process or later in the implementation, may authorize ATIMS to provide additional functionality, not supported by the current JMS or planned on the JMS roadmap. These modifications to the JMS code base, also known as additional "Enhancements" or "Customizations," will be provided in a manner consistent with the provisions of this SOW. This includes the change control, requirements gathering and specification, development, release, documentation, testing, and training processes.

All County authorized Enhancements will be entered into and tracked on the Requirements Traceability Matrix, with updates to other project artifacts as appropriate. Additional agreed to fees will be recorded and tracked on the Payment Schedule.

Design and Development

If any material software enhancements or customizations are required during this project to meet County requirements, ATIMS and the County will conduct a Joint Application Development (JAD) session to discuss and review requirements and design options. During or after the JAD session, ATIMS will provide the County with requirements and design documents for review. The County will provide feedback and signoff if the specifications meet the County's approval.

ATIMS and the County will cooperate on specifications and design to reconcile ATIMS need for a single code base with the County's needs and requirements. Any interpretations, details, assumptions, or clarifications made to produce an enhancement will be agreed to by the County and ATIMS.

The County will be responsible for ensuring the applicable business requirements and any related functional attributes have been clearly identified and are met prior to sign off on a requirement design specification.

To meet agreed on design specifications, should technical or functional incompatibilities arise, ATIMS will consult with the County to review options and design and capability tradeoffs.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

15) Modifications – Design Specifications	**Type: Document** **DED: YES**
Description	ATIMS, in cooperation with the County, will identify exact functional requirements to create specific functionality agreed to be provided by ATIMS and/or otherwise authorized by the County. These requirements

	will be used by ATIMS to create ATIMS design specification documents that will guide ATIMS technical development efforts. The process of developing design specifications will follow an iterative process, including at least one draft review cycle.
Requirements	1. A separate Design Specification document for each system modification, including: • Functionality description, including how the function differs from the current system. • Identification of data elements and related tables • Description of any business rules • Business process diagrams for complex functions • Screen/report mockups • Error handling 2. Updated process diagrams showing how the modified/new functionality will integrate with existing ATIMS JMS functionality and accommodate County processes.
Joint Activities	1. Establish functional requirements for each agreed upon modification/new function.
ATIMS Activities	1. Create a schedule of work sessions, and if necessary, agendas with input from the County, to review functionality requirements. 2. Provide questions to County regarding templates, reports, and functions. 3. Review County provided documentation 4. Conduct interviews with County staff regarding functionality requirements 5. Create a Design Specification Document for each functionality modification (function, screen, report, etc.).
County Activities	1. Participate in all analysis/work sessions. 2. Provide information as requested by ATIMS including sample data, documents, screenshots, policies, and procedures, etc. 3. Review and provide feedback on each Design Specification Document

Acceptance Criteria	1. Design Specification Documents comply with the requirements of the SOW and DED, and address the functionality agreed to be provided by ATIMS or authorized by the County.

Development of Modifications will occur in Track 5A) Build – Modifications.

TRACK 3C: Analysis – Interfaces

The objective of the Interface Track is to define the requirements (schema and other specifications), create an automated data sharing environment between the JMS and internal and external third-party systems (entities that are either receiving or sending data from/to County), test those interfaces, and resolve any errors.

Multiple interfaces are required for this project and are in scope [See RFP, Appendix A Technical Requirements and Exhibit L]. An interface to a data source may include multiple data exchanges. Interfaces may be one or bi-directional, real time, near-real time, or on demand.

ISE

It is required, unless otherwise noted in the RFP or agreed to by the County, that all interfaces will use the County's Information Sharing Environment (ISE) and it is the responsibility of ATIMS, with the assistance of the County as noted in the SOW, to create required interfaces between the JMS and third-party data stores via the ISE. ATIMS is responsible for transmission between the JMS and ISE and the County will be responsible for transmission between third party data stores and ISE. ATIMS is responsible for transmission between the JMS and any direct point-to-point third-party data stores. Interfaces will include authentication, secure transmission, business rule processing, and error handling acceptable to the County.

No custom or third-party integration tool will be provided by the County to accomplish input or output of data to/from the JMS. Exceptions to the ISE integration requirement, authorizing point to point interfaces, may be granted with the County's approval.

For JMS Interfaces, ATIMS shall provide API(s) or other method(s) for the JMS to provide data to or receive data from the ISE (i.e., expose the JMS interface to the ISE). ATIMS shall repurpose JMS APIs or other methods utilized in current ATIMS interfaces for use in County ISE data exchanges where practical and provide development where not.

Process

ATIMS shall provide an overview of interface capability and inventory of interface, tools, and methods available with the out-of-box JMS. ATIMS shall work with the County to identify existing APIs or other methods for the JMS to receive or provide data for each JMS Interface. For each JMS Interface, if existing JMS functionality cannot provide data from the JMS or receive data into the JMS required for a particular interface, ATIMS shall extend the JMS data structure to meet the SOW requirements at no additional charge. Modifications to the User Interface, including creation or modification of business rules, are subject to agreement by ATIMS and the

County and/or the Change Order process.

ATIMS shall follow the County's interface requirements, policies, and guidelines relating to standard data exchange format, communication protocol, authentication, and security.

ATIMS will develop the interfaces to meet the approved specifications for items included in the interface requirements and design. Upon completion of the application software and functional testing, the developed interface components will be incorporated into the JMS baseline to be used for system-level integration and testing. The County will conduct an acceptance test to verify that the interfaces meet County requirements and will provide a point of contact for any involved third parties.

The County shall provide assistance and information necessary for ATIMS to provide interface designs, development, and implementation. ATIMS will work with the County to map data elements including resolution of and where to place elements not supported by the JMS data schema.

During testing, County will work with ATIMS to identify mechanisms to simulate external agency systems and data should they not be available for testing.

ATIMS will meet with the County at the end of each development sprint to discuss testing, status and mitigation of any risks and issues.

Interface Control Document (ICD)
For each interface, ATIMS technical lead will work with the County's technical and business leads to document functional and technical requirements of the interfaces in an Interface Control Document. Interface development by ATIMS begins upon written approval of the ICD specifications.

ATIMS will update the ICD throughout the development and testing process as the process evolves.

Application / Agency Permissions and Assistance
The County's responsibility includes obtaining permission for the data integrations from appropriate application owners (including on premises or cloud/hosted, etc.). The County will ensure that ATIMS resources will have appropriate access to a Development or Test version of the ISE environment for interface and data exchange development.

The County shall provision services from third party providers of the interfacing systems if support activities or third-party system modifications are required.

Surveillance Use Policy

During the planning for integration of third-party data stores, the Sheriff's Office will conduct an analysis of any Surveillance Use Policies (SUP) of the interface source systems (e.g., ITS) to determine the Jail Management System (JMS) compliance with such policies, including the need to align JMS operations and policies to the third-party SUP or amend the SUP. The Sheriff's Office will consult with and seek guidance from the County Privacy Office and County Counsel on any potential SUP conflicts. Third party systems will not be integrated until the JMS is in compliance with relevant SUPs or a non-conflicting SUP is approved by the County of Sonoma Board of Supervisors

ATIMS Responsibilities:

- Develop interfaces according to approved ICD specifications to the source system as agreed to by the County in the ICD.
- If proper application documentation does not exist, work with the County to create the documentation. This may involve reverse engineering the interface.
- Execute all tasks including the setup of the interfaces between SCC and external systems in compliance with the ICD in an iterative process.
- Execute the transformation and rules that were used to map the legacy and target environments to include data clean-up tasks in an iterative process.
- Produce all necessary transaction monitoring capabilities to support the interfaces and data exchanges as detailed in the ICD.
- Provide assistance to County's creation of test case scenarios for interfaces.
- Conduct Function, Unit, and System testing of all interfaces
- Provide Error Reports of County responsible errors after each test and resolution of errors
- Update the ICD with any functional or design changes that are discovered during the design and test process to be advisable or necessary, and agreed to by the County.
- Provide a Weekly Interface specific status report.

County Responsibilities:

- Provide SME resources to work with ATIMS analysts throughout the Interface development and testing process.
- Participate in interface design specification workshops
- Facilitate communication with data exchange partner entities and their representatives.
- Provide access to systems to be integrated, including test environments.
- Provide and manage security access by ATIMS to third-party systems, including credential management.
- Assign a team of individuals with the ability to create/update/identify interface requirements; and experience designing, developing, and testing interfaces.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

16) Interface Plan	**Type: Document** **DED: YES**

Description	ATIMS and the County will conduct an analysis of interface requirements, ATIMS integration tools and methods, and County requirements, and develop an Interface Plan and Interface Control Documents (ICD) template that will guide interface development including script development and field mapping for the interfaces identified in the SOW and any newly identified Interfaces or changes agreed to by ATIMS and the County.
Requirements	The Interface and Data Exchange Specification Document shall include: 1. Design Guidelines & Approach 1) Glossary of Terms 2) Design Considerations 3) Assumptions, Constraints & Risks 4) Alignment with County ISE Architecture 2. Design Considerations 1) Development Methods & Contingencies 2) Architecture Strategies for County ISE Alignment 3) Data Exchange Performance Requirements 3. System Architecture & Architecture Design 1) Logical View 2) Hardware Architecture 3) Software / Tools Architecture 4) Information Architecture 5) Security Architecture 6) Performance 7) Full Integration Architecture Diagram 4. Interface & Data Exchange Design 1) Interface & Data Exchange Requirements 2) Database Impacts 3) Security Requirements

Joint Activities	1. Discuss and agree upon the Interface Plan including roles and responsibilities, components, methods, tools, approaches, etc. 2. Conduct business analysis workshops as necessary. This will require access to County personnel that has intimate knowledge of the individual data sources and business requirements the interfaces are to meet.
ATIMS Activities	1. Prepare an agenda and conduct an Interface Planning Workshop including the following topics: 1) Roles and Responsibilities. 2) Identification of targeted data sources including owners and access procedures. 3) Method of moving the data between data stores, including the format of the data (XML, ASCII, staging tables, etc.) 4) Direction of dataflow and frequency of exchange. 5) Data integrity, cleanliness, validation, and formatting issues. 6) Data mapping from one system to another. 2. Create a Data Interface Plan incorporating the Design Documents that describes the specific data sources to be interfaced, tools and methods, details of the interface (data elements, business rules, type of interface, method of transfer, error handling, etc.), and responsibilities of ATIMS and the County.
County Activities	1. Review the Surveillance Use Policy (SUP) for all interfaces and ensure the JMS is in compliance with relevant SUPs. 2. Provide authorization and cooperation from owners of each data source subject to an interface. 3. Provide appropriate documentation (including system screen shots and, if available, an entity relationship diagram and data dictionary) for existing interfaces. 4. Provide access to qualified application and technical staff members able to assist ATIMS during the interface process. 5. Provide data and data access from each data source in the format and manner specified in the Interface Plan. 6. Participate in workshop sessions. 7. Review and approve the Interface Plan

Acceptance Criteria	1. Planning workshops are held and an Interface Plan is created per the SOW and DED.

Development of the interfaces will occur in Track 5B) Build – Interfaces.

TRACK 3D: Analysis – Conversion

Overview

Data conversion is the collection of activities associated with the migration and transformation of data from the County's current legacy JMS to the new ATIMS JMS.

ATIMS will create a detailed Data Conversion Plan to govern the data conversion process. As part of developing the Conversion Plan, ATIMS shall work with the County to determine data to be converted and migrated from the legacy County systems. ATIMS shall develop and test scripts to extract data from source systems, transform data as required, and load data into the JMS. The County will provide the source data to ATIMS and ATIMS will perform data cleansing. ATIMS will run scripts against the County data to transform and load the data into ATIMS environments.

ATIMS shall migrate all current and historical data , or as specified by the County, from the current legacy system.

Conversion Process

The conversion process will move legacy data from the current JMS system(s) to the ATIM JMS database via an extraction, transformation, and loading (ETL) process. Below is a high-level view of the Conversion Process which will be detailed and updated, as appropriate, in the Conversion Plan.

Data Extraction – County will provide an extract of the legacy data ("source data") in a structured and agreed upon format where it will be imported into a raw SQL database by ATIMS. There will be multiple source databases.

Cleansing and Mapping - ATIMS will perform an analysis of the source data with the County to create a data map. The analysis will include the types of data to bring over, where it will reside within the ATIMS environment, how to handle inconsistencies in reference data, business process rules, any data integrity issues, and data cleansing processes.

Transformation - ATIMS will create a template database to be used as a starting point for every conversion. ATIMS will create programmatic scripts based on this analysis to convert the data. Once scripts are ready, for each conversion, ATIMS will create a new instance of the template database and run the scripts. The scripts pull from the source database, apply the conversion logic and output to the new instance of the template.

Load and Validate - ATIMS will validate the data load prior to giving it to the County. Typically, the SO will provide rosters and reports from the extracted source file they provided to be used for count validation and spot-checking data internally. The database, once validated, will be loaded in a test environment. County staff will have an opportunity to test and review sample data in the new system to check and ensure the data has been properly converted prior to final conversion and the scheduled system implementation 'Go Live' date. The County will determine the type of data (Live or Masked) to be used in the various environments.

Test Runs and Error Reporting

Pursuant to the Data Conversion Plan, ATIMS will execute multiple iterative test runs. Test runs may include partial data sets with each subsequent run including the data from the prior run. Acceptance of a test run requires County sign-off and agreement on the resolution of errors for that run.

After each test run, ATIMS shall provide data exception reports (in an Excel and/or SQL table format, as agreed to by the County), with remediation recommendations, including adjustments to the data conversion scripts or source system data corrections. ATIMS shall modify and adjust their conversion scripts as required before performing the next test data conversion.

ATIMS shall perform at a minimum two (2) full test data conversions without errors not excused by the County. A full test run is defined as including all data identified in the Conversion Plan to be migrated to the new JMS.

There is no formal limit to the number of full test runs that may be conducted as a test run with errors will require rerunning the test unless an error is excused by the County or the PMs agree to other remedial action. In addition, a full data transformation load is preceded by many smaller iterative conversions which increases the chances of the full load meeting expectations, these partial, iterative test runs are not counted in the full runs total.

Separately, ATIMS shall perform the final data conversion as part of the System Cutover Go Live process.

Inconsistent Legacy Schemas

Where there is a mismatch between the legacy and ATIMS JMS data schemas and County considered critical legacy data elements, or their functional equivalent, do not exist in the ATIMS schema, the PMs will review workarounds including repurposing ATIMS data fields. Data may also be mapped and concatenated into text fields. If these options do not provide rough equivalency of function, ATIMS will create up to 50 new columns (data elements) in their data structure at no cost. Any new business logic requested by the County related to the new data elements, unless otherwise agreed by ATIMS and the County (e.g., where the functionality is beneficial to other ATIMS customers), is subject to the change order process.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

17) Conversion Planning Workshop(s)	**Type: Meeting** **DED: No**
Description	The Data Conversion Planning Workshop(s) will provide a forum for ATIMS and the County to review the conversion process, roles, and responsibilities.
Requirements	The Conversion Workshop topics will include, but are not limited to: 1. Review of the Conversion process 2. Roles and Responsibilities 3. Identification of data sources including owners and access procedures

	4. Development of a thorough understanding of the data targeted for conversion. 5. Review of data access, format, integrity, and cleanliness issues 6. Determine and review the most effective means of performing the Data Migration. 7. Discuss and agree upon the Conversion Plan elements, requirements, approaches, and tools to be used.
Joint Activities	1. Discuss and agree upon Data Migration Plan elements and migration scope, timing, approaches, tools, issues, etc.
ATIMS Activities	1. Conduct data migration workshops to define code, parameter, and business rules for migrating legacy data to the new solution 2. Review ATIMS conversion process, tools, and recommendations with the County.
County Activities	1. Identify data to be migrated 2. Extract data from County legacy systems into ATIMS SQL databases reflecting the original source schema. 3. Populate import templates provided by ATIMS, if required, with ATIMS direction and assistance. 4. Provide legacy data in an agreed upon format, including wherever possible tables with readily identifiable keys and table record counts. 5. Provide source data business rules and any other information that clarifies data usage
Acceptance Criteria	1. Completion of the Planning Workshop(s) consistent with the requirements of the SOW and workshop agendas.

18) Conversion Plan	**Type: Document** **DED: YES**
Description	The Conversion Plan will identify County data sources required for migration, identify the process and responsibilities to convert County data sources to the ATIMS JMS data model, identify the data source dependencies, order, and priority of the conversion efforts to load County data to the JMS data repositories.
Requirements	The Data Conversion Plan will include: **Approach** 1. Clearly stated data conversion objectives

2. Identified ATIMS and County Assumptions
3. Roles & Responsibilities
4. Schedule
5. Identified Constraints
6. Risks

Data Cleansing Strategy

1. Cleansing Scope and analysis of existing data sources
2. Cleansing Approach (including automated and manual efforts)
3. Roles & Responsibilities
4. Cleansing Schedule
5. Cleansing Preparation (e.g., Sandbox Environments & Tools)
6. Cleansing Quality Assurance and Validation

Data Conversion Strategy

1. Scope
2. Approach
3. Roles & Responsibilities
4. Schedule
5. Quality Assurance and Validation

Plan Elements

The Conversion Plan must include, at a minimum, the following information:

1. Roles, Responsibilities, and Phases
2. Identification of County resources required to manually convert data or review the results of conversion activities in test or production
3. Process to be employed to monitor Plan activities
4. Processes to be used for validation, standardization, purification, and "deduplication" of the data. County and

	ATIMS staff will jointly make decisions regarding edit Incorporation of criteria, default values, and error exceptions. 5. SOW Migration Requirements 6. Identification of targeted data sources 7. Data transformation rules 8. Mapping templates and procedures 9. Methods (manual and automated) to extract, manipulate and insert the data 10. Step-by-step plan to move the data from source to target 11. Identification and development of reports used to clearly demonstrate that the load and all possible situations are handled properly to provide an audit trail for all the data loaded into the system 12. How errors will be detected, corrected and how users will be involved in this process 13. Error Report format 14. Data quality testing approach and clean-up plan 15. Contingency plan to roll-back data at Cutover should data migration – or some element – fail.
ATIMS Activities	1. Create & develop a detailed data migration plan that includes a comprehensive strategy for automated and manual data migration from County to ATIMS data stores. 2. Facilitate workshops to identify County specific requirements. 3. Conduct a readiness assessment with County staff as per the approved Data Migration Plan. 4. Publish the Detailed Data Migration Plan for County review and approval.
County Activities	1. Allocate and assign County SME resources to participate in workshop sessions. 2. Review & Validate the Detailed Data Migration Plans.
Acceptance Criteria	1. Delivery of the Conversion Plan consistent with the requirements of the SOW and DED.

19) Data Map	Type: Document DED: No
Description	The Data Map will document the relationship of data elements from the legacy system(s) to the JMS. ATIMS scripts will rely on the Data Map.
Requirements	The Data Map will include, at a minimum: 1. Legacy Table Name 2. Legacy Field Name 3. Inclusion Field ("Yes" If a Field is to be included in the migration) 4. JMS Table Name 5. JMS Field Name 6. Data transformation rules 7. Data business, validation, and exception rules 8. Complete database diagrams detailing the mapping of data sources to the System database.
Joint Activities	1. Conduct data mapping and business analysis workshops as necessary. This will require access to County personnel that have intimate knowledge of the legacy database layout and function 2. Discuss and agree on field mapping and business logic requirements for any data targeted for migration.
ATIMS Activities	1. Create a Data Map of legacy data elements to the ATIMS JMS, including business rules to transform data to match the new JMS configuration and reference codes as agreed by the County.
County Activities	1. Participate in Mapping workshops 2. Participate in the data mapping activity, mapping source data to staging format. 3. Provide appropriate documentation (including an entity relationship diagram, data dictionary, system screen shots and/or access to the current JMS) and access to qualified application and technical staff members able to assist ATIMS in mapping County data elements. 4. Provide to ATIMS information as requested. 5. Review and approve the Data Map

Acceptance Criteria	1. A Data Map is submitted by ATIMS, consistent with the SOW and Conversion Plan, that covers all legacy data systems and targeted tables.

Migration Test Runs will occur in Track 5C) Build – Migration.

F) PHASE 3: BUILD

TRACK 4: Configuration

The ATIMS JMS system, while a single code base, has been represented by ATIMS as a highly configurable system that can meet the business needs of different customers through its configuration architecture. Configuration includes the setting of JMS system parameters, codes, flags, functionality options, triggers, business logic, and table values to allow the JMS to conform to the SO business operations.

Common configuration examples include setting processing options, the operation of workflows, whether data fields on a screen are visible, the label attached to a field, and the values that display in a list of values (drop down).

As the JMS is built out with modified or new functionality, the system will be designed so that most, if not all, functionalities and activities required under this SOW can be accommodated through configuration to maximize flexibility and changing future needs.

To support the County's configuration of the JMS, ATIMS shall provide comprehensive documentation, including directions on how to manage/update current configuration values in updatable template worksheets, During Track 7 Training, ATIMS shall update system and project (e.g., RTM) documentation affected by configuration settings within 5 business days of relevant finalized changes to the configuration, or as agreed by the Project Managers.

Limitation, Constraints and Skill Sets
ATIMS will provide the system with default settings and reference (list of value) codes and the County, with ATIMS training, guidance, and assistance, will tailor or "personalize" the system to meet County operational requirements through the configuration settings. To establish these values the County will need to reassess their business operations and make numerous decisions on how they want the system to operate. This process will involve ATIMS SMEs who are deeply experienced with the JMS and jail management practices in other jurisdictions, and County SMEs who are deeply familiar with current business operations and the future state the SO desires to achieve.

The County understands that configuration of the system and access to Administrative functions, including responsibility for the setup and operation of the system, should be limited to County staff who will receive appropriate ATIMS Administrative training.

The County's JMS environments will be configured during the Configure Track of the Build Phase. ATIMS resources will configure the solution to align with and support County's required and desired business operations and train the County to manage the configuration of the JMS on an ongoing basis.

As the system is configured, ATIMS will demonstrate to County subject matter experts that the solution meets the County's requirements. Configuration settings, changes, and updates will be automatically populated across environments by ATIMS.

Configuration is an iterative process and the initial configuration completed during the Configure Track will be fine-tuned and updated throughout the implementation process.

Upgrades and Site Options

An example of configuration functionality is "Site Options." ATIMS has the ability to add site options that clients can turn on to access particular features of the software. ATIMS continually upgrades the JMS software to meet new client needs and improve upon current functionalities. Upgrades are provided to current ATIMS maintenance clients as they are developed and tested and become available for distribution. The County can decide -- via a "Site Options" feature -- whether to use them or not. ATIMS will not require the County to use these features upgrades and the upgrades will not impact County processes.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

20)Configuration – User Roles & Security	**Type: Software** **DED: No**
Description	ATIMS will set up several initial user accounts and related security permissions of the Core Team in advance of the Initial Core Team Training. ATIMS will provide training on how to create user accounts and related security permissions to allow County administrators to create accounts for the remaining County staff.
Joint Activities	1. Collaborate on the creation and configuration of user roles and security settings that will efficiently and securely meet SO business processes and meet project goals.
ATIMS Activities	1. Provide documentation to create and manage user accounts and security settings 2. Conduct one or more User Roles & Security training Workshops 3. Ensure configuration settings are reflected in the JMS documentation and training program. 4. Configure the JMS application to meet County approved configuration specifications.

County Activities	1. Review User Roles & Security documentation 2. Conduct internal reviews and assessments to determine appropriate user roles and security settings. 3. Participate in User Roles & Security Workshops 4. Review, test & validate the application configuration settings and builds as they are released throughout the implementation by ATIMS .
Acceptance Criteria	1. Completion of required User Roles & Security Workshops 2. Provision of all User Roles & Security documentation including manuals and worksheets 3. Successful creation of County required User Roles & Security accounts and settings. 4. Ability of the County to successfully manage and modify User Role and Security configuration settings.

21)Configuration – System Administration	**Type: Software** **DED: No**
Description	ATIMS includes high-level system administrative (global) settings that determine how the JMS will operate.
Joint Activities	1. Collaborate on the creation and configuration of system administration settings that will efficiently and securely meet SO business processes and project goals.
ATIMS Activities	1. Provide documentation to manage JMS administrative settings 2. Conduct one or more Administrative training Workshops 3. Ensure configuration settings are reflected in the JMS documentation and training program. 4. Configure the JMS application to meet County approved configuration specifications. 5. Create additional system admin documentation as needed for the County to understand how to successfully manage and modify administrative settings.

County Activities	1. Review System Administration documentation 2. Identify County preferences among JMS system configuration options 3. Participate in the System Administration Workshops 4. Review, test & validate the application configuration settings and builds as they are released throughout the implementation by ATIMS.
Acceptance Criteria	1. Completion of required System Administration Workshops 2. Provision of all System Admin & Technical configuration manuals and worksheets 3. Ability of the County to successfully manage and modify administrative configuration settings.

22)Configuration - Modules	Type: Software DED: No
Description	The ATIMS JMS includes a number of sub modules (e.g., Intake, Classify, Programs) that can be configured to accommodate SCC business practices. ATIMS will provide documentation and workshops to ensure the SO has a complete understanding of each JMS module and function.
Joint Activities	1. Collaborate on Module configuration and Workflow requirements and functionality that will improve SO business processes and meet project goals.
ATIMS Activities	1. Provide JMS Module documentation. 2. Conduct configuration training workshops for each module. 3. Ensure configuration settings are reflected in the JMS documentation and training program. 4. Configure the JMS application to meet County approved configuration specifications. 5. Demonstrate the JMS to confirm configuration updates are working to specification.
County Activities	1. Review Module and configuration documentation 2. Conduct internal meetings with SO SMEs to review SO business processes and determine which configuration settings are advisable or necessary and their related business logic requirements. 3. Participate in the Module Configuration Workshops 4. Review, test & validate the application configuration settings and builds as they are released throughout the implementation by ATIMS.
Acceptance Criteria	1. Completion of necessary Module Workshops 2. Provision of all Module and Workflow documentation including manuals and worksheets 3. Ability of the County to successful manage and modify Module configuration settings.

TRACK 5A) Build - Modifications

Details of the design and development process are provided in Track 3B) Analysis – Modifications. Following is the deliverable for Track 5A) where the development of the Modifications specified in Track 3B are built.

23)Modifications - Development	**Type: Software** **DED: No**
Description	Upon acceptance of the Design Specification documents by the County, ATIMS will begin and complete development as agreed to by the PMs.
Requirements	ATIMS is to develop and test modifications and new functional requirements as authorized by the SOW and/or agreed to by ATIMS and the County.
Joint Activities	1. Agree to a sprint development and release schedule.
ATIMS Activities	1. Develop modified/new functionality per the Design Specifications. 2. Provide weekly status updates specific to development of any modifications. 3. Conduct Unit Testing and resolve any errors 4. Release modified/new functionality per the release schedule for County to test 5. Provide release notes for any modified/new functionality 6. Conduct a Training workshop for the County regarding any new modified/new functionality, including a demo and walkthrough. 7. Provide support to County and resolve any functionality issues reported by County.
County Activities	1. Test modified/new functionality as ATIMS provides releases 2. Report any issues to ATIMS
Acceptance Criteria	1. JMS functions properly, per the Design Specifications, without Severity Level 1, 2, 3 or 4 Defects.

TRACK 5B) Build - Interfaces

Details of the interface design and development process are provided in Track 3C Analysis – Interfaces. Following are the deliverables for Track 5B) where the development of the interfaces specified in Track 3C are built.

24) Interface Control Documents (ICD)	**Type: Document** **DED: YES**
Description	The ICD is a design specification document for an individual interface. The ICD will describe the interface, data elements and mapping, rules for processing, messages within the JMS, validation rules, exception processing, alerts, logging, testing plans, and acceptance criteria.
Requirements	Create an Interface Control Document (ICD) for each identified Interface, that shall include, at a minimum: 1. Schema of data to be received from County Agencies and ancillary systems 2. Schema of data to be submitted to County Agencies and ancillary systems 3. Specific JMS configuration requirements to support data integration 4. Integration flow 5. JMS adapter/connector type (e.g., web service, file, etc.) 6. Interface content (field descriptions) 7. Interface trigger event and frequency 8. Validations and exception processing 9. Testing process and considerations 10. Business processes affected 11. Business rules (detail) 12. Message format and sequence

	13. Data elements to be exchanged 14. Privacy/Security Requirements 15. Direction (outbound/inbound) 16. Data transformations and translations 17. Testing requirements and Testing Plan for each interface (Unit, Function and System Tests). Tests will include data sent and received, data transformations, the business rules and/or workflows triggered by the messages sent and received, and error handling, including a graceful exit.
Joint Activities	1. Conduct business analysis workshops as necessary. This will require access to County and third-party personnel that has intimate knowledge of the individual data sources and business requirements the interfaces are to meet 2. Review and agree on field mapping and business logic requirements for any interface.
ATIMS Activities	1. Provide workshops to identify and validate County specific requirements. 2. Create Interface Control Document(s), with County provided input. 3. Publish the Interface Control Document(s) for County review and approval. 4. Review and update the Interface Control Documents based on feedback from the County.
County Activities	1. Allocate and assign County SME resources to participate in workshop sessions. 2. Review & Validate the Interface Control Document(s). 3. Update and implement required data sharing agreements and MOUs with external agencies as per approved ICDs as to access, specifications, development, schedule, and cost. 4. Provide requested information and feedback as needed. 5. Review and approve each individual Interface Control Document (ICD)

Acceptance Criteria	1. An ICD is created for each interface and the ICD conforms to the Interface Plan and ICD DED.

25) Interface Development & Testing	Type: Software DED: No
Description	The objective of this deliverable is to develop, test, and deploy the SOW specified individual interfaces between the JMS and ISE (or as otherwise agreed) to the ICD specifications.
Requirements	1. Develop (including extending functionality as necessary), configure, and deploy the JMS Interface engine and tools to meet County interface requirements, including transmittal of data to and from the ISE. 2. Develop and deploy interfaces and data exchanges to County requirements 3. Configure Interface security to County requirements
ATIMS Activities	1. Create and review with the County an interface development schedule with firm sprint dates 2. Develop the JMS Interfaces per ICD specifications. 3. Deploy and publish the JMS Interfaces for County review and approval. 4. Develop scripts, programming and procedures that will allow the receipt of data from a third-party data source to the JMS and/or the transfer of data from the JMS to a third-party source meeting the technical and business requirement specifications in the ICDs. 5. Perform Interface Testing in cooperation with the County for each designated interface. Testing shall be conducted per the Interface Plan and will include the processes for ATIMS and the County to perform data validation. Iterative testing will be required to ensure the interface meets DED requirements. 6. After conducting interface testing, provide a status report to the County on the tests, including issues requiring County assistance. 7. Update the Interface Design documents and Interface Plan as necessary with updated procedures, business rules, and other instructions needed to document the interface process. 8. Perform complete regression testing on all previous deliveries.
County Activities	1. Cooperate with ATIMS in support of the data interface efforts. 2. Allocate and assign County SMEs to participate in validation sessions. 3. Create programming as necessary to assist in the interface process.

	4. Develop test plans and procedures based on the interfaces' designs. 5. Conduct acceptance testing for each interface, reporting errors, and providing acceptance when the interface is successful as defined in the IDD. 6. Review the Interface Test results. Inspect and validate the data to determine adherence to the Interface Plan and ICD.
Acceptance Criteria	1. Each of the SOW interfaces meets the SOW and ICD specifications and runs without error.

TRACK 5C) Data Migration

Details of the design and development process are provided in Track 3D) Analysis – Migration. Following are the deliverables for Track 5C) where the test runs of the data migration analysis and planning efforts specified in Track 3D occur.

26) Test Runs (ETL)	**Type: Software** **DED: No**
Description	The objective of this task is to migrate County data per the SOW, Data Migration Plan, and Data Map specifications. Multiple iterative test runs are required.

Requirements	**Conversion Development Activities** 1. Conduct analysis of existing data sources for cleansing and mapping. 2. Develop scripts, programming, and procedures that will allow the transfer of data from the legacy system to the JMS. **Test Run Execution** The Data Conversion Test Run deployments shall include but not be limited to: 1. Data Extraction and Staging 2. Data Transformation and Loading 3. Migration 4. Error Reports 5. Error Resolution **Error reports** Error Reports will be generated after each test run and, at a minimum, include: 1. Number of successful rows converted by table 2. Number of error rows by table 3. List of error rows by table, including, the record identifier and the failed data element, process, or rule, and a description of the error

Joint Activities	1. Agree to the number, form, content, and scheduling of test runs. 2. Conduct a review of the Migration Testing process and test results, modify procedures including data test/validations, business rules, data mapping, and update the Data Migration Plan and Data Maps as necessary.

ATIMS Activities	1. Extract - Execute and for all identified data sources to maximize accuracy, eliminate inappropriate or redundant data, provide default values where needed, and perform other actions as appropriate. 2. Load - Run scripts to move the data from staging to a test environment 3. Transform - Transform data to the correct values and format per the Conversion Plan and Data Map. 4. Publish the Data Conversion builds for County review and approval to schedule. 5. Iteratively conduct data migration tests to ensure the migrated data is in compliance with the data map. 6. Provide an Error Report detailing all data that fails the conversion process after each test run, including failure to load, inconsistent formatting, null values, duplicate keys, etc. 7. Review Error Reports with the County, document issues and resolution activities, and modify ATIMS scripts as necessary. 8. Rerun the Test until errors are resolved or County conditionally accepts the results with a mutually agreed upon mitigation plan. 9. Update the Conversion Plan and Data Map as appropriate with procedures, business rules, and other instructions needed to guide the migration process.
County Activities	1. Allocate and assign County SMEs to participate in validation sessions. 2. Provide data or access as requested by ATIMS subject to adherence to security requirements. 3. Provide table control numbers. 4. Review, Test & Validate the Data Conversion test iterations as they are released. 5. Review the Test Migration, including inspecting and validating the data to determine adherence to the Data Map, reporting any data or business process issue to ATIMS.

	6. Assist with data cleansing activities in accordance with the Data Migration plan.
Acceptance Criteria	1. In alignment with the SOW and Conversion Plan, legacy data is able to be migrated to a JMS environment with no unresolved errors. To resolve errors the County may modify the scope of the conversion or (conditionally) accept the error.

27) Final Conversion Report	Type: Document DED: No
Description	At the end of the conversion test process, once two (2) full test runs have been executed without error, ATIMS will provide a Final Conversion Report summarizing the conversion activities.
Requirements	1. The Final Conversion Report, at a minimum, will include: 1) Listing of all test data conversions completed 2) Final test data conversion results, including summary and detail data exception reports 2. Update the Conversion Plan with Go Live elements to include Failover and Recovery testing and procedures at least one (1) month in advance of the scheduled Go Live date.
ATIMS Activities	1. Prepare and deliver the Final Conversion Report 2. ATIMS will warrant that it will immediately correct (within 12 hours or as agreed to by the County) any Data Migration related failures identified by the County caused by a failure to adhere to the Data Migration Plan or Data Map.
County Activities	1. Review the Final Conversion Report.
Acceptance Criteria	1. The Final Conversion Report, including all updates, is delivered consistent with the requirements of the SOW and Conversion Plan,

TRACK 5D) Forms & Reports

Forms

A form is one or more data entry screens that emulates a paper-based form/document (and/or the document itself) that also can be exported in a PDF and is generally a person-based document (e.g., intake form, medical clearance form, classification form). A Form must be able to pull, reference, and display data previously entered into the JMS as well as structured and unstructured (free form) text entered by the user.

Requirements:

1) County staff will be able to copy and modify JMS forms to create new forms.
2) Forms must be able to be printed (PDF) and downloaded).
3) ATIMS will create, according to County specifications, up to ten (10) custom electronic Forms, not including the pre-book arrest form, the medical pre-screening form, and the classification and re-classification forms, selected by the County, at no additional cost., including Forms identified in Appendix D: Requirement Fees.
4) ATIMS will provide initial training to allow the County to create additional forms. to the County.
5) The County may elect for ATIMS to create additional forms at an agreed upon fee.

Reports

A report may have a tabular format and/or provide calculated values and may include tables and charts. Reports should have multiple selection and sorting criteria, and include grouping, subtotal, and total functionality. A Report, built with the ATIMS JS Report tool must be viewable from within the application and can be printed and exported.

Reports can also be generated by applications such as SSRS, Power BI, Crystal Reports, etc. and accessed outside the application.

Requirements

1) ATIMS will provide all system standard reports (current and future) to the County, with accompanying documentation, at no charge.
2) County staff will be able to copy and modify JMS Standard reports to create new reports.
3) Reports must be able to be filtered, printed, and downloaded. County will review the standard reports and, for reports that do not export to CSV or Excel, notify ATIMS whether the report, per the SOW Excel/CSV requirement, must be modified to export to Excel or. CSV.
4) ATIMS will create, according to County specifications, up to ten (10) custom reports, selected by the County, at no additional cost, including Reports identified in Appendix D: Requirement Fees.
5) ATIMS will provide training to allow the County to create additional reports at no cost to the County.
6) The County may elect for ATIMS to create additional reports at an agreed upon fee.

Dashboards

Intuitive data visualizations (charts, graphs, dashboards, and drilldowns) for each major functionality area (including Search) are required to provide real-time, accurate, and consumable information necessary to support internal decision-making at all levels (shift supervisors, facility leaders, specialty units, and command staff).

Reporting Environment

ATIMS will deploy the JMS application reporting environment, including real time or near real time access to production data, as agreed to by the County, which shall include, but is not limited to:

1) Reporting Server and Infrastructure
2) Self-Service, User and Administrator standard dashboards, forms, and reports.
3) ATIMS Form and Report creation tools including third party software and licenses as necessary (e.g., JS Reports).
4) Custom Forms and Reports as specified by County.
5) Administrative tools

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

28) Forms Specifications	Type: Document DED: YES
Description	A Form Design Specification document will provide the requirements for each form to be created by ATIMS
Joint Activities	1. Review and collaborate on County form needs to identify which forms should be created.
ATIMS Activities	1. Provide Form template guides and directions for the County to assist ATIMS in creating Form Specification Documents. 2. Create a Form Specification Document for each report ATIMS is to create.
County Activities	1. Review existing forms to create a master Go Live list, excluding forms that are duplicative, no longer in use, or are defective 2. Identify required and representative forms for ATIMS to create that can serve as a model for the County to use to create similar forms 3. Assist ATIMS in creating required Form Specifications including required data elements, business rules, and format.
Acceptance Criteria	1. The Form Specification Document captures the County's desired requirements.

29) Forms Development	Type: Software DED: No
Description	ATIMS will create new Forms as provide by the SOW.
ATIMS Activities	1. Develop new Forms per the Form Specification Documents provided by the County 2. Respond to and Resolve Errors and issues as reported by the County. 3. Update the Form Specification Documents as changes are made.
County Activities	1. Review and test existing and new Forms created by ATIMS as they are released. 2. Report Errors and issues and retest
Acceptance Criteria	1. The JMS is able to generate required Forms, pursuant to the Form Specifications, without error

30) Reports Specifications	Type: Document DED: YES
Description	A Report Design Specification document will provide the requirements for each report to be created by ATIMS
Joint Activities	1. Review and collaborate on County report needs to identify which report should be created.
ATIMS Activities	1. Provide Report template guides and directions for the County to assist ATIMS in creating Report Specification Documents. 2. Create a Report Specification Document for each report ATIMS is to create.
County Activities	1. Review existing reports to create a master Go Live list, excluding forms that are duplicative, no longer in use, or are defective 2. Identify required and representative reports of high, moderate, and low complexity, for ATIMS to create that can serve as a model for the County to use to create similar forms 3. Assist ATIMS in creating required Report Specifications including required data elements, business rules, and format.
Acceptance Criteria	1. The Report Specification Document captures the County's desired requirements.

31) Reports Development	Type: Software DED: No
Description	ATIMS will create new Reports as provide by the SOW and as agreed to by ATIMS and the County.
ATIMS Activities	1. Develop new Reports per the Report Specification Documents 2. Respond to and Resolve Errors and issues as reported by the County. 3. Update the Report Specification Documents as changes are made.
County Activities	1. Review and test existing and new Reports created by ATIMS as they are released. 2. Report Errors and issues to ATIMS and retest
Acceptance Criteria	1. The JMS is able to generate required Reports, pursuant to the Report Specifications, without error

TRACK 6: Testing

This section summarizes the overall test approach to be used to accept software modules, functions, and services during the implementation. Specific testing activities may be the responsibility of ATIMS, the County, or a joint responsibility as noted in the SOW and DEDs.

Throughout the implementation, progressive test cycles shall be repeated until all bugs and anomalies are resolved and the system components are demonstrated to meet all applicable criteria, specifications, and testing requirements.

All testing by ATIMS or the County will follow the Acceptance Process and Issue Resolution Process (See Section C Acceptance Process).

ATIMS Testing

ATIMS - Functional Testing

ATIMS functional testing confirms that the configuration and system functions applied to the Test environment are operating correctly. ATIMS functional testing is performed during the Build phase upon delivery of a specific component such as a software function or interface.

During ATIMS Functional testing, the system is tested to:

- Confirm the system meets JMS baseline specifications and documentation
- Confirm that the system configuration is correct and meets the requirements documented in the RTM.
- Validate the requirements scheduled to be met in the release
- Identify defects and add to the development queue to be addressed in the next release

JMS functionality is validated against

- Project Requirements per the RTM
- ATIMS documentation
- Enhancement design documents

ATIMS – Interface Testing

Interface testing is performed during the Construction phase. ATIMS executes and manages interface testing with support from client personnel who are familiar with the source and target systems.

Outbound Interfaces

Testing for outbound interfaces ensures that events in the JMS are executing correctly, that messages are created in the appropriate format and routed correctly. Per ATIMS, program routines are used to acquire outbound data and to validate the contents, format, and (if relevant) routing and metadata information.

Inbound Interfaces

Per ATIMS, testing for inbound interfaces is simulated by program routines that send a message to ATIMS Online for processing. The Routines will create valid and invalid messages to ensure that interface logic appropriately manages any error conditions.

ATIMS - System Testing

System Testing verifies and validates that the JMS is performing as expected with migrated data.

System testing utilizes test cases that were successfully executed and passed in the previous functional testing. These test cases are run again, this time on a preproduction environment that combines system elements already verified and validated by functional testing with migrated data.

During ATIMS system testing, the JMS is tested to:

- Confirm that the system elements that were tested and passed during functional testing, continue to operate as expected in a different environment with migrated data
- Confirm that business scenarios work with migrated data

Testing objectives are verified and validated using the following documents and requirements:

- Project requirements as stated in the RTM
- Enhancement design documents and Enhancement functional test cases
- ATIMS documentation

ATIMS - Performance Testing

Performance testing begins as soon as possible during the Construction phase, after the JMS is configured in the proposed TEST and PROD environments and is also performed during the Transition phase. Performance testing ensures that the JMS can support the expected number of users and active inmates while maintaining reasonable response times (per System specifications and the Performance Testing plan).

ATIMS shall execute the developed performance test plan to ensure that the system will meet all response-time requirements when deployed to all users and used during peak workloads. ATIMS shall tune and otherwise update the system to resolve noted issues. ATIMS shall repeat stress- test cycles until all issues are resolved. To support Disaster Recovery, ATIMS will conduct failover and recovery testing to ensure that the high availability and business continuity goals are met.

Custom datasets and migrated data will be used for performance testing.

Performance testing includes:

- Load testing - Executes a concurrent user load and/or a system load on a simulated "live" fully operational system, at incremented concurrency ramp-up rates, to determine system stability, performance, and integrity. The testbed includes offender and user data, reference data, workflow

queues, tasks, and business rules. During load testing, system components are monitored and correlated with transaction response times.

- Soak Testing - Verifies that the JMS can maintain a specified level of user concurrency for an extended period of time with no degradation over time.
- Stress Testing - Measures the JMS performance at upper workload limits and verifies that the system recovers when the workload is reduced.

Performance testing will also include monitoring the database - disk I/O, memory usage, CPU utilization, and network usage which will be measured against a County provided baseline.

Performance metrics will include, at a minimum, the following RFP standards:

- During the peak usage hour of the peak usage day, 98% of online transactions are completed<1 second
- 99% of all online transactions are completed <= 1 second
- 99% of dashboard results display <= 1 second (results will paginate)
- 95% of reports generate <=10 seconds

ATIMS and the County may agree to modify the performance testing methods and metrics.

Maintaining an ATIMS SaaS environment that meets security, performance, business continuity, and administrative requirements, is a material condition of this statement of work. Significant or continued issues with, or failure to meet these requirements, in the sole judgement of the County, will trigger a review of the project by the County addressing causes and remediation, including consideration of an On-Prem environment.

ATIMS - Regression Testing

As part of the above tests, ATIMS will perform on-going regression testing to ensure functionality has not been negatively impacted by integration with other systems, changes to configuration, or updates to the JMS solution.

County Testing

During the implementation the County will perform several types of testing.

County - Functional Testing

The County performs functional testing throughout the implementation to verify that the JMS, as configured by ATIMS and the County, performs per ATIMS specifications and County requirements.

During County functional testing, the JMS is validated against:

- Project Requirements per the RTM
- ATIMS documentation
- Enhancement design documents

County – End to End Interface Testing

The County will rerun the test cases originally run by ATIMS during system testing and interface testing. During the Transition phase, the test cases are performed on the Test environment that has all of the interfaces configured. ATIMS team members will support the County's testing efforts.

County - End to End Data Migration

The County will rerun the test cases originally run by ATIMS during system testing and data migration testing. During the Transition phase, the test cases are performed on the Test environment with the migrated data. ATIMS team members will support the County's testing efforts.

County - User Acceptance Testing (UAT)

UAT is performed during the Transition phase by the County with assistance from ATIMS, after Functional, End to End Interface and End to End Data Migration is successfully completed.

UAT uses real client resources to simulate real business scenarios to test that the ATIMS system behaves as anticipated and can support client business processes. Interfaces and migrated data are also tested during UAT to verify that the JMS performs to the SOW specifications.

The County will have a minimum of two (2) months to conduct the initial UAT period, the exact time period to be determined by the County during the creation of the Test Plan. The initial UAT period may be extended by the County as necessary to ensure successful completion of the UAT.

UAT will use the existing System Test Cases already developed by ATIMS and the County in addition to specific User Acceptance Test Cases developed to extend beyond already completed testing.

If a Severity Level 1, Level 2 or Level 3 Defect (See p. 46) is identified, and such Defect has a material impact on continued UAT progress so as to stop or substantially slow down the UAT process until a resolution is provided, the UAT period for that Defect, the testing it is affecting from completion, and any additional Severity Level 1, 2 or 3 Defect, which would not have been identified through testing as a result of the initial Defect blocking, will be extended.

In each case, the parties will:

- assess the magnitude of the reported defect and the timeline required to provide resolution
- determine the appropriate period of time needed to re-test, including regression testing
- determine a mutually agreeable revised project schedule that may incorporate an extension to the UAT period and, if appropriate, an extension to the project period of performance.

User Acceptance Testing is completed once the end-to-end solution is validated by the County Testers.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

32) Acceptance Test Plan (ATP)	Type: Document DED: YES
Description	The ATP will identify and document the test strategies, process, workflow, tools, and methodologies to validate the JMS build against the County requirements.
Requirements	The objective of this task is to create a detailed Acceptance Test Plan that will govern ATIMS and County testing activities. **ATP Workshop** ATIMS and the County will conduct an ATP Workshop to review the ATP process and the following items: 1. Role and responsibilities 2. Roles and security requirements of the testers 3. Acceptance Test Checklist 4. Test script format and content 5. Pre-requisites for each test/script including identification of any system parameters, settings, and data fields that require validation. 6. Expected results for each test/script 7. Issue reporting 8. Communication process during testing

	9. Release management **Detailed Test Plan(s):** The ATP will include: 1. Unit/module testing approach 2. Systems integration testing approach 3. County user acceptance testing approach 4. Performance and stress testing approach 5. Security testing approach 6. Test data creation approach, including data refresh processes 7. Automated test usage (optional) 8. Defect remediation release strategy 9. Defect reporting and tracking
ATIMS Activities	1. Develop the Detailed Test Plan(s) with County provided input. 2. Facilitate workshops to identify County specific requirements, use cases, process flows, and procedures required to define a successful test that proves the requirements have been met as expected. 3. Publish the Detailed Test Plan(s) for County review and approval
County Activities	1. Allocate and assign County SME resources to participate in workshop sessions. 2. Review & Validate the Detailed Test Plan(s).
Acceptance Criteria	1. The ATP is comprehensive and provides for fully testing all facets of the JMS including existing and new functionality. 2. The ATP conforms to the requirements of the SOW and DED

33) System Testing	Type: Software DED: No
Description	End-to-end testing of the JMS functionality and reports after completion of all system modifications, interfaces, migration data testing and before UAT.
Joint Activities	1. Agree on the System Testing dates 2. ATIMS and the County will jointly create a set of at least forty (40) detailed automated test scripts, or the number necessary, as determined by County to comprehensively test each module's functionality to execute business use cases covering core JMS functionality, as determined by the County.
ATIMS Activities	1. ATIMS initiate System Testing after the completion of the Tracks 4, 5A, 5B, 5C, 5D
County Activities	1. Coordinate and enforce issue/defect management process for all County test activities 2. Respond to testing related queries from ATIMS 3. Review and approve Use Case Scripts as adequate to test the functionality of each module. 4. Attend test activity-related meetings with ATIMS, as required
Acceptance Criteria	1. Completion of a performance test exit report Outstanding performance transactions that are proven to not meet the service level agreements are declared in an exceptions list and included in the performance test exit report, with the County's agreement on each exception and logging of a defect as appropriate 2. No outstanding Severity 1 defects 3. No outstanding Severity 2 defects 4. No outstanding Severity 3 or 4 defects without a County approved resolution plan
	3.

34) Performance Testing	Type: Software DED: YES
Description	Performance Testing is conducted to ensure the JMS can support the expected number of user and inmate records.
Requirements	**Performance Plan** ATIMS and County will develop a performance and load test plan that defines data loads, potential bottlenecks, system activities, testing criteria and testing metrics. **Scripts** Scripts created for System Testing will be used in the performance tests. Test scripts will simulate a load of up to 2,000 simultaneous users conducting numerous system activities, including but not limited to creating new records, updating existing records, performing system searches, executing workflows, and executing business rules. **Test Types** Performance Testing will include: 1. Load testing 2. Soak testing 3. Stress Testing 4. Database and system testing (including disk I/O, memory usage, CPU utilization, and network usage) **Failover and (Disaster) Recovery Testing** Failover and Recovery Testing ensures that the system can successfully failover and recover from a variety of hardware, software, or network malfunctions with undue loss of data or data integrity.
Joint Activities	1. Review and agree on the performance test process, parameters, record sets and data, and simulated number of users and records.
ATIMS Activities	1. Execute performance tests to meet County performance benchmarks and metrics 2. Track performance-related issues 3. Provide a Performance test Exit Report detailing all test results

County Activities	1. Assist ATIMS with user script development. 2. Coordinate and enforce issue/defect management process for all County test activities 3. Respond to testing related queries from ATIMS 4. Attend test activity-related meetings with ATIMS, as required
Acceptance Criteria	1. Completion of a performance test exit report Outstanding performance transactions that are proven to not meet the service level agreements or County performance metrics are declared in an exceptions list and included in the performance test exit report, with the County's agreement on each exception and defect logging. 2. No outstanding Severity 1 defects 3. No outstanding Severity 2 defects 4. No outstanding Severity 3 or 4 defects without a County approved resolution plan

35) User Acceptance Testing (UAT)	Type: Software DED: No
Description	Also known as end-user testing, user acceptance testing (UAT) is where SO end users will test the software to determine whether it can be accepted or not.
Requirements	**UAT Scope** 1. Functional tests that cover all published functions and features of ATIMS documentation 2. Functional tests that cover the functional and nonfunctional requirements identified in the RTM Functional tests that cover the identified business scenarios 3. Tests that cover the successful migration of data Functional tests that cover the identified interfaces 4. Tests that cover the integration of all software components identified in the contract specifications 5. Failover tests 6. Performance tests that cover the specifications for load and failover **Create UAT Checklists and Scripts.** The purpose of the UAT Checklists and scripts is to document and business requirements and processes. UAT scrips should include real-world scenarios using converted data, and include: 1. UAT Test Script ID 2. Function / Module 3. Test Title 4. Description 5. Pre-conditions 6. Dependencies 7. Test Steps 8. Test Data

	9. Expected Results 10. Post Conditions 11. Actual Results 12. Tester 13. Status (pass, fail) 14. Retest dates and results 15. County Final Decision (Acceptance, failure, or waiver) **User Acceptance Test Report:** The objective of this task is to document the Final UAT test results that prove the readiness for production go-live. The UAT Acceptance Test Report shall include: 1. Testing Scope 2. Testing Metrics 3. Test Summaries by Testing Type 4. Test Summaries of Environments and Tools 5. Defect Summary by Classification (Critical, High Priority, etc.)
ATIMS Activities	1. Provide System and Integration tests as a foundation for UAT 2. Assist developing the UAT Plan 3. Provide a base UAT Checklist and example scripts 4. Manage the UAT Environment 5. Support the UAT by reviewing the UAT Log and responding to questions and issues 6. Develop and compile the Final UAT Test results. 7. Publish the Final Test Report for County review and approval.
County Activities	1. Ensure UAT Testers receive appropriate training and instruction before testing begins 2. Complete functional configuration of the system (e.g., reference code values and related parameter settings) before UAT 3. Create appropriate test data and use cases if needed beyond the Use Cases Scripts created by ATIMS 4. Maintain testing logs and triage user reported issues before reporting an issue to ATIMS

	5. Identify and provide SME testers who have sufficient knowledge of the system to adequately test the JMS 6. Develop UAT scripts 7. Execute the scripts and perform testing per the UAT Plan 8. Document results and attach supporting documentation (screen shots, etc.)
Acceptance Criteria	1. User Acceptance Testing Complete 2. All deliverables have been accepted based on Deliverable Acceptance quality criteria specified in Deliverable Expectation Documents (DEDs) 3. All Severity Level 1, 2 and 3 have been closed 4. Remaining Defects are considered acceptable by the County based on an ATIMS remediation plan.

36) Final Test Report	**Type: Document** **DED: No**
Description	The Final Test Report aggregates the findings of all previous test reports.
	The Final Test Report shall include: 1. A listing of County approved test results 2. Dashboard Summary of Previous Test Metrics 3. Test Summaries by Testing Type
ATIMS Activities	1. Develop and compile the Final Test Report. 2. Confirm the aggregation of all previous test summaries and reports. Summarize previous test metrics and validate recommendation for User Acceptance Testing to the County. 3. Publish the Final Test Report for County review and approval.
County Activities	1. Review, Validate and Accept the Final Test Report.
Acceptance Criteria	1. The Final Test Report meets the ATP criteria.

PHASE 4: TRANSITION

TRACK 7: Training

Overview

ATIMS will provide several types of training to assure that the County is able to fully utilize the JMS, including:

- Initial Training of the Core Project Team
- Training as part of the configuration workshop sessions
- Admin and Technical Training (for System and Database Administrators, as well as technical resources to assist with data conversions and interfaces)
- Train the Trainer Training (T3) (for "Super-Users")
- End User Training assistance
- Follow-up (Refresher) Training
- Mentoring
- Agency Forms and Report Writing Training

Initial Training of the Core Team, Administrative training, Train the Trainer training, and assistance with the initial End User Training will be onsite, details to be described in the Training Plan.

Requirements

1. ATIMS will prepare and execute a detailed training plan to identify the approach, methods, content, and activities associated with all project training.
2. Train the Trainer (T3) training will be completed by a to be determined date to ensure sufficient time for the County to conduct end-user training.
3. Training shall be conducted on-site; however, training may be changed to remote learning on agreement by the County.
4. Each training class will provide exercises and testing to assess the knowledge gained and to evaluate the effectiveness of training course delivery.
5. ATIMS shall coordinate with the County Training Manager to use best efforts to adhere to County training standards, guidelines, and best practices.

Workshops

Workshops are facilitated by ATIMS subject matter experts for small groups of participants and focus on functional areas of the JMS solution. Workshops are an interactive learning environment where participants accomplish a number of training activities according to a pre-arranged workshop agenda. These sessions are less formal than instructor-led training, but the smaller class size and focused agenda is intended by ATIMS to provide participants an in-depth, hands-on learning experience.

Courses

Details on course offerings (subjects, number, length, etc.) will be provided in the Training Plan.
The County is expecting a structure and class sessions that will include, but are not limited to:

- Basic Jail System Training Sessions
- Advanced Jail System Training
- Jail Administrator & System Support Training

Train the Trainer (T3)

ATIMS will develop performance-based, customized training content and will utilize a T3 approach to train County instructors to deliver end-user training. In addition to functional instruction on the JMS, County training resources will receive coaching and guidance on how to train others from ATIMS Trainers. County Trainers will be given supplemental material (e.g., job aids and training guides) to assist them in training delivery. The purpose of this approach is to create a sustainable training platform that can continue in-person training once the project is completed.

ATIMS will train at least 8 teams of 5 Jail staff members, or the functional equivalent**,** who are qualified and designated as "Super Users". After training, the super users will be knowledgeable of all modules of the JMS and be able to resolve issues or identify problems regardless of their current position or assignment. Super users will in turn train County end users.

Materials for T3 training will include, at a minimum for each module, an Instructor Training Guide, handouts for end users, and a Module Overview video (10-15) minute video outlining system functionality and screen layout) may be replaced, at County option, with County videos.

End User Training (EUT)

The County is responsible for End User Training, however, ATIMS will assist by:

1) Reviewing and providing assistance with the development of the County's EUT Plan.
2) Providing instructor assistance, if requested, to assist with and shadow the Trainers initial EUT classes.

Onsite Requirements

On site trainers must adhere to County Health (e.g., Covid-19) and Security requirements.

Training Materials
Throughout the implementation, ATIMS will deliver appropriate training materials at least two weeks before any class or training session for the County's review.

Documentation

Documentation consists of creating, developing, revising, maintaining, reproducing, and distributing information in electronic and hardcopy forms. ATIMS will provide updated System Documentation on an on-going basis.

Requirements

1. Documentation will be available in the JMS Online Reference system and in PDF or Word.
2. County is authorized to make unlimited copies for County's internal use.
3. ATIMS will maintain and update documentation to reflect software feature and functionality updates.
4. County created documentation can be incorporated into the JMS Online Reference Help system and updated by the County.
5. Documentation will contain screenshots of all screens with a narrative description of all displayed fields.
6. ATIMS provided training materials will be tailored to reflect the specific configuration of the County's JMS.

Documentation Types
ATIMS shall provide documentation specific to the County's JMS implementation, including, but not limited to Product use and technical materials, for trainers, end-users, administrators, and technical resources.

Product User Documentation
The Product User Documentation will describe the operation of the product from the perspective of the end user. The Documentation will cover sign on and sign off, menus and navigation, functional operations, screen descriptions, reports and forms, workflow, wizards, user security and permissions, online help, and other system functional topics.
Documentation will include:

- High Level JMS and Major Component Overviews
- Manuals (for the JMS and all components and modules), including screen shots with related descriptions and explanatory detail
- Video Recordings
- Error Code Directory (for the JMS, components, and reports), including error explanations
- Standard Report and Form List (including screen shots, narrative descriptions of all displayed fields, input parameters, and execution directions)

- Workflow and Wizard Guides/Manuals, including descriptions, diagrams, and details for each included workflow and wizard

User manuals will provide sufficient depth and clarity to enable users to utilize all relevant system features in the course of their work duties.

Administrative & Technical Documentation

ATIMS will provide technical documentation of sufficient depth and clarity to enable County IT and technical personnel to:

- Perform all system administration and operation duties (including system setup and configuration)
- Understand the underlying structure, function, and operation of system components (including system maintenance, error management, backups, disaster recovery, and performance specifications)
- Troubleshoot the application software and interfaces (including platform, network, and security interfaces)
- Support users (Level 1 Helpdesk)
- Manage security and user accounts
- Support integration with other applications

Technical Documentation includes:

- System Architecture Overview and Diagrams
- Data Dictionary
- Entity Relationship Diagrams
- Interface engine, toolkit, and API documentation
- Business Continuity Runbook

Administrator Documentation includes:

- System Administration and Security Manuals
- Configuration and System reference code values
- Ad Hoc Report and Form Creation Manuals
- Workflow Diagrams

Other Documentation

Project Management Documentation (e.g., the Project Management Plan and related plans) as well as specific deliverable documents (Data Migration Plan, Go live Plan, etc.) are detailed elsewhere in this SOW.

ATIMS shall provide release notes and update functional and technical documentation (system manuals, ERD

diagrams, etc.) when a new Update is issued. In addition to a list of included JIRA tickets, Release Notes will include screen shots of any UI changes with changes highlighted or called out and accompanied by a description of the change/update.

ATIMS will conduct a walkthrough of changes when an Update is issued and, upon request by the County, when patches or new builds are released.

The table(s) below provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

37) Training Plan	**Type: Document** **DED: YES**
Description	The Training Plan defines the training objectives, content, scope, approach, deliverables, resource requirements, scheduling, and critical success factors. It describes in detail what the training requirements for the solution are and how the training will be delivered, as well as any risks or constraints inherent in the training delivery.
Requirements	At a minimum the Training Plan will contain the following: 1. Training Objectives (learning objectives) 2. Training Scope 3. Training Requirements 4. Training Approach (e.g., Train-the-Trainer) and Methods 5. Training Deliverables (training materials, etc.) 6. Resource Requirements (trainers, training rooms, equipment, etc.) 7. Training Schedule (including attendees and locations) 8. Training Evaluation (pre-post assessment materials) 9. Critical Success Factors
Joint Activities	1. Establish a training schedule that meets ATIMS and County resource availability in alignment with the Project Work Plan.
ATIMS Activities	1. Provide a Training Plan draft based on ATIMS experience and in accordance with the SOW. 2. Update the Training Plan based on County comments. 3. Create a Training Syllabus (course outline) for each session or course including the session objectives and topics. 4. Review the County's End User Training Plan and provide feedback

County Activities	1. Collaborate with ATIMS on training elements, including approach, topics and content, schedule, resource requirements, and required training materials 2. Identify the number of users to be trained and type of training required 3. Confirm availability and scheduling of staff, training rooms, and equipment 4. Review, Validate and Accept the Training Plan
Acceptance Criteria	1. The Training Plan meets the SOW and DED requirements and incorporates County feedback.

38) Training Documentation	**Type: Document** **DED: No**
Description	ATIMS will supply and develop as needed, training materials and aids to be provided to County Trainers to facilitate their training of end -users.
Requirements	Training materials, for each module, will include, but are not limited to: 1. Instructor Training Guides 2. Overview/Quick Start Guides 3. Video recordings 4. Exercise Guides (scenarios, step by step use cases)
Joint Activities	1. Review training materials for completeness and suitability
ATIMS Activities	1. Develop and provide training materials 2. Configure online help content to incorporate the most recent documentation and County specific content.
County Activities	1. Review training materials for completeness and suitability.
Acceptance Criteria	1. The Training materials are complete, of sufficient detail to explain JMS concepts and functionality, and suitable for use by the County Trainers to train end-users.

39) Forms Training	Type: Training DED: No
Description	ATIMS will provide training on the use and management of existing standard JMS Forms and the design, specification, and development process to modify, copy, and create new forms.
ATIMS Activities	1. Provide Training workshops on existing JMS Forms, Form Management, and Form creation.
County Activities	1. Assign County SME's to participate in Form training and design specification sessions.
Acceptance Criteria	1. The training sessions are complete, County attendees have graded the sessions satisfactory or better, and the County is able to modify and create JMS Forms.

40) Reports Training	Type: Training DED: No
Description	ATIMS will provide training to County SMEs on the use and management of existing standard JMS Reports and the design, specification, and development process to modify, copy, and create new reports
ATIMS Activities	1. Provide Training workshops on existing Reports, Report Management, Permissions, Reporting tools, and Report creation.
County Activities	1. Assign County SME's to participate in Report training and design specification sessions.
Acceptance Criteria	1. The training sessions are complete, County attendees have graded the sessions satisfactory or better , and the County is able to modify and create Forms.

41) Admin & Technical Training	Type: Training DED: No
Description	ATIMS will provide administrative and technical training.
Requirements	ATIMS Administrative and Technical training will be detailed and sufficient to allow County administrative and technical staff to: 1. Perform all system administration and operation duties (including system setup and configuration), 2. Understand the underlying structure, function, and operation of system components (including system maintenance, error management, backups, disaster recovery, and performance specifications), 3. Troubleshoot the application software and interfaces (including platform, network, and security interfaces), 4. Support users (helpdesk), 5. Manage security and user accounts, 6. Support integration with other applications.
Joint Activities	1. Schedule train-the-trainer sessions
ATIMS Activities	1. Provide ATIMS instructors with advanced product and training experience. 2. Ensure the training environment is prepared for training 3. Deliver Training to County Administrators and technical staff 4. Provide training materials
County Activities	1. Provide training rooms and necessary equipment as per the training plan 2. Track attendance at train-the-trainer sessions 3. Resolve attendance conflicts and schedules with the trainers 4. Distribute Training Evaluation Surveys to attendees to elicit feedback regarding the quality, content, and scope of the training they have received.
Acceptance Criteria	1. The training sessions are complete and were conducted according to the SOW and Training Plan. 2. County Trainers have graded the sessions satisfactory or better.

42) Train The Trainer (T3)	Type: Training DED: YES
Description	ATIMS will deliver onsite training to trainers as per the Training Plan to prepare trainers to deliver end user training. The training will be sufficient to allow County trainers to provide appropriate training to County end users. Sessions will be led by an ATIMS trainer with assistance from County Core Team members who completed the Administrator training. The ATIMS instructor will provide detailed knowledge of the JMS application and the SO trainer, familiar with SO business policies and procedures, will assist in the training and explain, as appropriate, the reasoning behind the SO configuration and plans to use the JMS.
Requirements	1. TT3 training will be provided for at least 8 teams of 5 staff members, or the functional equivalent.
Joint Activities	1. Collaborate on required courses (topics, content, number, prerequisites) and scheduling. 2. Ensure the training database is loaded with the latest configuration and sufficient data to use in exercises
ATIMS Activities	1. Provide ATIMS instructors with significant product and training experience. 2. Ensure the training environment is prepared for training 3. Deliver Training to trainers on how to deliver training on the solution 4. Provide training materials to trainers (electronically) 5. Present the software in a manner that will facilitate an interactive exchange with the SO Trainers to: a. Ensure attendees understand the functional use of the software. b. Establish that attendees have the knowledge to successfully train others. c. Resolve common training problems to minimize disruption and delays that may be expected during the end user training process.

	6. Monitor attendance and ensure attendees receive appropriate training. 7. Provide a Training Assessment to the County a. Assessing the attendee's ability to understand the material, b. Identifying any areas that need further training, c. Detailing in writing any issues regarding training delivery
County Activities	1. Provide training rooms and necessary equipment as per the training plan 2. Ensure attendees have appropriate user accounts and security permissions. 3. Assign, schedule and ensure attendance and participation of Core Team members, who have previously completed the Admin Training, to assist the ATIMS Trainer. 4. Assign, schedule and ensure attendance and participation of appropriate staff for training sessions 5. Resolve attendance conflicts and schedules with the trainers 6. Track attendance at train-the-trainer sessions 7. Provide staff roster of attendees to ATIMS in advance of training. 8. Distribute Training Evaluation Surveys to attendees to elicit feedback regarding the quality, content, and scope of the training they have received.
Acceptance Criteria	1. The training sessions are complete and were conducted according to the SOW and Training Plan. 2. County Trainers have graded the sessions satisfactory or better.

43) End User Training (EUT)	**Type: Training** **DED: No**
Description	The purpose of end user training sessions is to provide the knowledge required to use the JMS for daily SO business activities, processes, and procedures. The main purpose is to cover subjects geared toward the business functionality of each individual Unit or Participant Group. For that reason,

	training sessions are customized to provide the right level and type of content based on the users that are attending. The County Trainers will conduct End User training for all SO staff who will be users of the JMS
ATIMS Activities	1. Review and assist with the County's development of an EUT Plan 2. Provide trainers to assist/shadow the County trainers for their initial EUT sessions. 3. Ensure the test database is loaded with the latest configuration and sufficient data to use in exercises.
County Activities	1. Create an EUT Plan including objectives, process, materials, attendees, classes, schedule, requirements, limitations, risks, and methods to test attainment of EUT goals. 2. Schedule end-users for EUT. 3. Provide training facility with appropriately configured desktops and workspace for trainers and environment for instructor (desktop, projector, whiteboard) 4. Ensure attendees have appropriate user accounts and security permissions. 5. Assign, schedule and ensure attendance and participation of appropriate staff for training sessions 6. Schedule follow-up training as necessary. 7. Distribute Training Evaluation Surveys to attendees to elicit feedback regarding the quality, content, and scope of the training they have received.
Acceptance Criteria	1. EUT was conducted in accordance with the requirements of the SOW and Training Plan.

44) Final Training Report	**Type: Document** **DED: No**
Description	ATIMS will create a Final Training Report at the conclusion of EUT to provide a summary of provided training and recommendations.
Requirements	The Final Training Report will include: 1. A summary of all training provided, including course, date, and attendees. 2. A summary of training exercise results and trainer readiness.

	3. General observations of completed training, details of any training issues, and future training recommendations 4. A Training Assessment assessing the attendees ability to understand the material and identifying any areas that need further training,
ATIMS Activities	1. Create and deliver the Final Training Report.
County Activities	1. Review the Training Report and provide comments.
Acceptance Criteria	1. The Final Training Report is complete in accordance with the requirements of the SOW and DED

TRACK 8: Go Live

Deployment Strategy

As part of the Go Live Plan, the ATIMS PM Team shall work with the County to determine the approach for rolling out the JMS including phasing strategies and site-specific considerations. ATIMS shall conduct workshops with County stakeholders to determine the deployment strategy and include consideration of benefits and risks of strategy alternatives.

Final Acceptance Testing (FAT)

Final Acceptance Testing is the last set of tests performed by ATIMS and the County, preceding a Go / No-Go decision and commencement of production use of the JMS.

ATIMS will devise, and the County will approve, a formal test plan. The County will monitor and approve results of tests conducted before JMS acceptance.

The County and ATIMS will sign and date all testing results and will agree on whether or not the JMS passes FAT or needs more modification and/or testing.

If the County determines that the JMS does not pass FAT, the County shall notify ATIMS in writing, and ATIMS shall modify or correct the JMS as required at no additional cost to the County.

Acceptance testing will be completed when ATIMS and the County agree that the JMS is ready for production, and when both parties sign, date, and mark the final acceptance on the testing forms.

Production Environment

ATIMS shall install all application components, establish the initial system configuration, load initial data per the Data Conversion Plan and perform any other activities required for production usage of the JMS. ATIMS shall support the County for any cutover activities restricted to County staff. ATIMS shall test the production system prior to system go-live.

ATIMS shall conduct one (at a minimum) Tabletop Rehearsal cutover to confirm the process and to establish the cutover timeline.

ATIMS shall provide enhanced Go Live Support (over and above ATIMS Hyper and standard support) during the pre, post, and cutover period as follows:

- Onsite Go Live support shall be provided for a minimum of 14 calendar days or as agreed to by the County.
- Once ATIMS staff are onsite, the Go Live support period will be extended, at no additional cost to the County, should production use of the JMS be delayed, or require a restart, for at least the period of delay, unless otherwise agreed to by the County.
- The ATIMS PM will provide onsite management of the ATIMS cutover process and resources from the day before the final migration cutover to the release, by the County, of onsite staff.
- ATIMS is required to have onsite staff, from the final migration cutover day to day 10 of production use, who can provide functional expertise, including assistance with the data conversion and interfaces.
- Onsite ATIMS staff will be subject matter experts in the use of the County's JMS and the configuration of the JMS by the County.
- ATIMS will provide 24x7 onsite support staff, not counting the PM, at each of the County's two facilities, starting on the day of the final migration cutover and extending for 10 days after production use of the JMS commences.
- Upon the 6th day of production use, ATIMS may reduce onsite coverage to two (2) onsite staff, not counting the PM, each covering a twelve -hour shift, or as otherwise approved by the County, coverage shift start/end times to be determined.
- Onsite staff will be stationed at, or otherwise travel between, the County's two facilities as determined by the County.
- The County may reduce or otherwise ease the onsite requirements depending on the performance of the JMS and ability of County staff to operate the JMS without the need for onsite assistance.
- County's assent is necessary for the release of onsite ATIMS staff.

ATIMS shall update the Configuration Management Plan with the go-live production configuration.

ATIMS shall apply industry best practices and work with the County to determine recommendations for managing organizational change required for the JMS to meet the project objectives. Such recommendations shall be developed considering business impact on each of the JMS stakeholder groups.

Go – Live Criteria

The County shall make its decision to "Go Live" (begin production use of the JMS) based on the Go Live Plan and in consultation with ATIMS, however, the decision to Go Live is solely the choice of the County.

The following is a preliminary list of Go-Live criteria for assessing the JMS and County readiness for Go Live, to be finalized during Track 8 Go Live.

1. **System Functionality** – The ATIMS solution configured in support of the JMS Implementation meets the functional and operational requirements as specified in the Fit/Gap Analysis and as evidenced by the County's acceptance of UAT. Additionally, the system will be accepted for operation use when it satisfies the following four (4) requirements:
   - No Severity Level 1 issues
   - No Severity Level 2 issues
   - All Severity Level 3 issues have workarounds identified, agreed with the County, and communicated to users
   - All Severity Level 4 issues identified, agreed, and documented

2. **Data Readiness** – Data migrated from source systems to ATIMS has completed QA and satisfies the following four (4) requirements:
   - No Severity 1 Level issues
   - No Severity 2 Level issues
   - All Severity 3 Level issues have workarounds identified, agreed with the County, and communicated to users
   - All Severity 4 Level issues identified, agreed, and documented

3. **Reporting** – All reports identified elsewhere in the SOW to be completed by ATIMS have been tested and accepted by the County. Acceptance criteria are:
   - No Severity 1 Level issues
   - No Severity 2 Level issues
   - All Severity 3 Level issues have workarounds identified, agreed with the County, and communicated to users
   - All Severity 4 Level issues identified, agreed, and documented

4. **User Readiness** – All affected County departments have completed the training according to the Training Plan in order to prepare them to use the JMS solution on Day 1 of production use , including:
   - All classroom training completed per the Training Plan
   - County personnel have received soft copies of all finalized training materials

5. **Operational Readiness** – Support infrastructure, equipment, tools, and procedures are in place and ready for use. Operational staff are trained (user and system administration). Technical support staff are in place and prepared to handle reporting, prioritizing, and fixing problems.
    - Planning, Help Desk, and Change Control processes in place
    - User and System Administration training completed per Training Plan
    - Knowledge Transfer post go-live to System Admins

6. **External Factors** – Interfacing Organizations/Departments, stakeholders, and affected staff have been communicated with, and the County is ready for launch

7. **Go Live Plan** – The Go Live Plan is developed and accepted by business owners, and has been vetted via a dry run so that any potential gaps are identified and resolved prior to go-live
    - User Support – User support requirements are defined and accepted by the County for the three (3) month post go-live support period. All post go-live ATIMS support staff are named and identified at least two (2) weeks prior to go-live
    - Process for capturing, logging, and resolving operational issues during the post go-live support period is documented and agreed upon
    - The Support escalation process is documented and agreed upon

The below table(s) provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

45) Go Live Plan	Type: Document DED: YES
Description	Prepare a Go Live Plan finalizing a Go Live date and including functional, technical, and business process checklists.
Requirements	Collaborate, create, and deliver a Go Live Plan, including the following topics: 1. Go/No Go decision process 2. Go/No Go Checklist 3. Final Migration 4. Cutover Prerequisites & Criteria 5. Technical deployment of the system 6. Issue reporting 7. Contingency / Rollback Strategy 8. Assignments and schedule for County and ATIMS staff 9. Communication activities and procedures
Joint Activities	1. Prepare a Pre-Go Live Checklist 2. Prepare a Go/No Go Checklist 3. Prepare a Go Live Checklist
ATIMS Activities	1. Develop the Cutover Plan framework. 2. Facilitate workshops to validate County specific requirements, identify risks and develop mitigation paths. 3. Publish the Cutover Plan for County review and approval
County Activities	1. Allocate and assign County SME's to participate in requirements and risk mitigation workshops. Review, Validate & Approve the Cutover Plan. 2. Ensure the County Team is fully committed to the Go Live Event and proper governance and leadership is in place to guide the County through a successful Go Live. 3. Plan, schedule, communicate, and coordinate all user planning, preparation and go live tasks and events. 4. Review the Go Live Checklist and provide comments.

Acceptance Criteria	1. Delivery of a Go Live Plan in accordance with the requirements of the SOW and DED.

46) Go Live Preparation	**Type: Activity** **DED: No**

Description	Conduct preparation meetings, review, and complete any outstanding work and issues, ensure the environment, software and staff are ready for Go Live.
Requirements	**Pre-Go Live Check List** Execute the Pre-Go Live Checklist **Install Latest JMS Version** Install the latest version of the JMS software to the production environment with all related updates and fixes to provide required functionality and resolve system errors. 1. Perform system and environment stabilization assessment(s). 2. ATIMS shall provide prompt notice to the County of any technical infrastructure or application deficiencies. **Update User & Technical Documentation** Develop and deliver all JMS solution documentation maintained to the current component versions identified as production release candidates and publish the System Documentation for County review and approval. Documentation will include: 1. End User Documentation 2. System Administration Documentation & Guide 3. Environment, Data Management and Maintenance Documentation 4. Interface and Data Exchange Documentation **Go Live Checklist and Readiness Report (Go- No Go)** During the Go Live Preparation period, ATIMS and the County will complete the Go – No Go Checklist which will be used to make a final decision on whether or not to Go Live. 1. Create and develop go/no go cutover criteria, steps, and stage gates

	2. Report findings and recommendations prior to cutover and report on situations that will impede successful cutover and provide mitigating measures. 3. Coordinate remediation actions based on readiness assessment findings.
Joint Activities	1. Update the Data Migration Plan with Go-Live Plan elements to include Failover and Recovery testing elements at least one (1) month in advance of the scheduled Go-Live date. 2. Verify the operational readiness of the production environment. 3. Execute the Pre-Go-Live Readiness Checklist 4. Review the Actions Agreements, Issues and Risks (AAIR) Register to ensure all applicable actions, issues and risks have been addressed. 5. Create a Go Live Contact List with emergency numbers.
ATIMS Activities	ATIMS shall plan and conduct activities required to begin production use of the JMS and verify the operational readiness of the production environment including: 1. Technical environment 2. Software Release and functionality 3. Failover and Recovery testing 4. Configuration 5. Interfaces 6. Reports and Forms
County Activities	1. Schedule, communicate and coordinate all user planning, preparation and go live tasks and events 2. Review readiness assessment and mitigating measures to provide feedback and approvals 3. Review and provide iterative feedback and approve cutover criteria including all steps and stage gates 4. Per the Go Live Plan, review and approve final Go/No-Go authorization for final cut over
Acceptance Criteria	1. The Data Migration Plan has been updated such that the Go-Live and Failover plans are considered by the County to be achievable, reasonable, and complete.

47) Go Live Conversion Cutover	Type: Software DED: No
Description	Prior to Go-Live ATIMS will coordinate necessary actions with the County to perform a final migration of SO data per the Conversion Plan.
Joint Activities	1. Conduct Final Migration Prep sessions.
ATIMS Activities	1. Conduct a thorough readiness/preparedness assessment against the cutover criteria. 2. Execute the Go Live Data Migration per the Data Migration Plan. 3. Manage and coordinate the cutover process to ensure that there is no or minimal break in service between operating the old and the new system 4. Resolve any stabilization/post cutover issues identified by ATIMS or County as highest priority within 24 hours of cutover.
County Activities	1. Assist ATIMS per the Data Migration Plan and as requested. 2. Verify successful migration of the data in the production system.
Acceptance Criteria	1. Successful completion of the Final Data Migration per the Data Conversion and Go Live Plans. 2. The JMS is fully functional and meets all agreed upon Go Live functional and technical requirements as specified per the SOW and Go Live Plan.

48) Go Live – Onsite Support	Type: Activity DED: No
Description	Go Live is the commencement of production use of the JMS application. Essential to Go Live is the successful cutover (Final Data Migration) of the County's legacy data.
Joint Activities	1. During the Go Live period, conduct Daily Review Sessions regarding the system's operation
ATIMS Activities	1. Provide the PM and sufficient onsite staff to support the County Go Live per the SOW. 2. Conduct a Go Live Preparation Meeting. 3. Execute the Go Live Checklist. 4. Support Go Live activities and assistance onsite. 5. Notify the County PM of onsite staff arrivals and authorized departures.
County Activities	1. Provide SME staff for each department to assist with Go Live and serve as the first line of support during the Go Live Period. 2. Issue Go Live Announcement to the County Departments and affected end users. 3. Conduct Pre-Go Live Preparation Meetings of County staff. 4. Commence operational use of the software in consultation with ATIMS and in accordance with the Go Live Plan. 5. Provide a detailed list of issues and questions that require resolution or explanation by ATIMS at the end of each day during the Go Live period. 6. Excuse ATIMS onsite staff as appropriate per the SOW and once their presence is no longer required by the County.
Acceptance Criteria	1. ATIMS staff is on site in conformance with the Go Live Plan 2. Daily Review Sessions are conducted

49) Transition to Support	Type: Meeting DED: No
Description	Upon Final Acceptance, ATIMS will conduct a turnover from Project Management to the ATIMS Support Department. ATIMS will provide appropriate management and technical staff to support the continued effective operation and maintenance of the JMS.
Joint Activities	1. Participate in an ATIMS Customer Support Turnover Meeting.
ATIMS Activities	1. Provide a Customer Support Turnover Packet in advance of the Customer Support Turnover Call. 2. Provide resources available to support the County on an on-going basis per the terms of the Support Services Agreement, including Hyper Care immediately following Go Live for a period of at least 30 days which includes proactive technical support and continued administrative and functional support by the Project Manager and implementation team
County Activities	1. Arrange the attendance of appropriate County staff including those responsible for ongoing system administration.
Acceptance Criteria	1. Completion of the Turnover Meeting

TRACK 9: Post Go Live

During the implementation, the County, in consultation with ATIMS, may decide to defer certain deliverables until after the system is Live in Production. Any deferred work will be memorialized in writing, including change orders and updates to the RTM and SOW, as appropriate.

The below table(s) provide a detailed description of each related deliverable, including the deliverable type (e.g., software, document,) and if a DED is required (e.g., Yes, No).

50) Post Go Live Deliverables	**Type: Software** **DED: YES**
Description	Post Go Live work typically may include specific modifications, interfaces, data migration and reporting requirements. Reporting requirements are often scheduled for post Go Live to allow the SO time to accumulate sufficient data in the new system to test and report. Interfaces, if they are new, is another example of work that is often deferred to post Go Live.
Requirements	Notification from ATIMS to the Sheriff's Office that Post-Go Live Deliverables are Complete fulfilling all SOW requirements, including: 1. Delivery of the latest Licensed Software version 2. Delivery of remaining Software Modification(s) 3. Delivery of remaining Interface(s) 4. Delivery of remaining Reports, Forms, and Dashboards 5. Delivery of Post Go Live Data Migration
Joint Activities	1. Conduct Post Go Live Review Meeting to review remaining work.
ATIMS Activities	**Software Modifications & Interfaces** 1. Provide post Go Live deliverables, including software modifications and/or interfaces, as detailed in the SOW or Post Go-Live Plan. 2. Assist the County to implement software modifications and/or interfaces as appropriate. 3. Provide training for software modifications and/or interfaces as appropriate.

	4. Perform Final Acceptance Testing in coordination with the County. 5. Resolve any Testing issues pursuant to the Test Plan process **Reporting** 1. Provide consultation, guidance, support and/or additional contracted services as appropriate to support the SO's data submission requirements as agreed to in the SOW. Assistance may include infrastructure and related operational environment review, configuration modifications, report modifications, spot training. **Data Migration** 1. Completion of Test Runs for remaining record sets to be migrated. 2. Resolution of migration script errors.
County Activities	**Software Modifications & Interfaces** 1. Assist ATIMS as detailed in the Post Go-Live Plan. 2. Provide resources and work with ATIMS to support the installation of new version releases and software upgrades when available. 3. Coordinate access to third parties as requested by ATIMS to install, update, and test any interfaces 4. Test software modifications and/or interfaces 5. Perform Final Acceptance Testing in coordination with ATIMS. 6. Provide timely approval of each software modification and/or interface **Reporting** 1. Provide report and form specifications 2. Provide staff as necessary to answer any ATIMS questions 3. Test reports and report any errors **Data Migration** 1. Test the Post Go Live Data Migration to validate for accuracy and completeness.

	2. Report errors to ATIMS
Acceptance Criteria	1. Completion of the Post Go Live Review Meeting. 2. Delivery and Acceptance of all remaining work.

51) Post Implementation Evaluation Report	Type: Document DED: YES
Description	ATIMS will perform an analysis of the implementation and create a Post Implementation Evaluation Report (PIER). The PIER report will include Lessons Learned, as well as an assessment of the use of the JMS by the SO and recommendations for future actions ATIMS and the County should consider to take advantage of the JMS capabilities. Lessons Learned is the knowledge gained during a project that shows how project events were addressed or should be addressed in the future for the purpose of improving future performance.
Requirements	The PIER should contain at a minimum: 1. Information that has been collected throughout the project on what has and has not worked 2. Information collected during facilitated project reflection sessions 3. A survey of County team members on the project implementation 4. Recommended improvements, tools, and techniques that can benefit future projects
Joint Activities	1. Agree on PIER content and structure.
ATIMS Activities	1. Facilitate reviews with the County to contribute to project reflections, identify and present best practices for County operation of the JMS solution.
County Activities	1. Allocate and assign County SME's to participate in review sessions, provide documentation and input as needed. 2. Review and validate the PIER.
Acceptance Criteria	1. Completion of the PIER per the requirements of the SOW.

TRACK 10: Project Close

Project Close is the final step in the Transition Phase. During Project Close the project managers will review the contract and Project Plan to confirm all deliverables and services have been successfully deployed per the terms of the SOW.

52) Project Close	**Type: Meeting** **DED: No**
Description	The ATIMS and County Project Managers review the project with County Executive Management, closes out all remaining tasks and disengages from the project. Project Closure formally confirms that the provision of ATIMS software and services have been completed. From this point forward, ATIMS and the County shall operate in a support relationship as provided for in the Support Agreement.
Requirements	1. All deliverable signoffs are complete 2. The post go-live stability period is complete 3. The Post Implementation Evaluation Report (PIER) ("Lessons Learned") document is complete. 4. The transition to the County's Information Services Division application support organization (i.e., the TSS) is complete
Joint Activities	1. Participate in Project Closure Review Meeting to review final project status to ensure all contracted products and services have been delivered and invoiced.
ATIMS Activities	1. Complete and/or provide any remaining deliverables or documentation.
County Activities	1. Complete any remaining payments due to ATIMS 2. Submit a Project Closure Letter to ATIMS
Acceptance Criteria	1. Completion of the Project Closure Review Meeting

Appendix A: Definitions

Term	Definition
AAIR Register	Actions, Agreements, Issues and Risks Register. A Workbook that includes separate sections to record and manage Action Items, Agreements/Decisions, Issues, and Risks.
Acceptance	(same as Formal Acceptance)
Acceptance Test Plan	A document describing the procedures and objective test criteria demonstrating that a Deliverable or Work Component (e.g. report, form, configuration, enhancement) meets required specifications.
Acceptance Criteria	Standards to be met to achieve deliverable requirements.
Activity	An activity or task is a work element that is generally considered necessary for completion of a Deliverable but is not itself subject to acceptance.
ATIMS	The Act 1 Group, Inc - dba as ATIMS
Business Day	A work-day (Monday through Friday) as defined by the County of Sonoma business calendar.
Change Order	A signed Change Request authorizing a change in deliverables, process, or requirements that may affect cost, scope, and/or timeline.
Change Request	A document to record requested changes to the project, including a description of the change, justification, and expected impacts.
Component Testing	Component Testing focuses on a specific piece of work and also is executed for those functional areas that are affected by a given release. Any component containing either a bug fix or some level of re-factoring shall be tested.
Configuration	The setting of system parameters, codes, business logic, table values, and work flow, including utilization of ATIMS event and interface engines and custom queues.
County	The County of Sonoma, California
Cutover	The transition of the JMS into production use, including the migration of legacy data to the production system.
Data Conversion/Migration	The movement and transformation/application of business rules to a set of data from one data store to a different data store.
Data Dictionary	Information about a database that defines its tables, fields, field types, field lengths, field definitions, and relationship to other tables.
Data Map	A document defining the relationship of data elements from the County's legacy JMS systems to the ATIMS JMS.

Day/Days	Unless noted otherwise, a “day” equals one calendar day
Deliverable	A Deliverable is a distinct piece of work product that can be individually examined for completeness, accuracy, quality, and acceptance. Examples of deliverables include: project documentation, status reports, software modules or functions, and other defined work.
Deliverable Expectation Document (DED)	Provides additional clarification and description of the deliverable that goes beyond the limited text in the SOW. The DED may elaborate on format, methodology, scope, artifacts, deliverable timing, and acceptance criteria.
Deliverable Signoff	County formal acceptance of a project deliverable
Documentation	The user guides/manuals, templates, specifications, workbooks, online help, release notes, videos, training materials and other instructional materials provided or made available by ATIMS to the County regarding the use, operation, and administration of the JMS.
Entity Relationship Diagram (ERD)	A graphical representation showing the relationships of entity sets (data tables) stored in a database, including table keys and linkage between the tables.
Error	A malfunction in the JMS and/or failure to meet JMS specifications and Documentation, which degrades the JMS or the County's use of the JMS.
Failover and Recovery Testing	Failover and Recovery Testing ensures that the test target can successfully failover and recover from a variety of hardware, software or network malfunctions without undue loss of data or data integrity
Final Acceptance	Provided by the County at the end of a 90 day post Go Live stability period without Severity 1 or 2 errors and confirmation, via a System Final Acceptance document from ATIMS, of the completion of all SOW requirements.
Formal Acceptance	Acceptance by the County of a Software/Project Deliverable or related work, pursuant to the SOW Acceptance Process.
Functional Requirement/Specification	A statement that describes what the system, process, function, or product/service must do to fulfill specific functional (business) or non-functional (technical) requirements.
Function Testing	Testing that focuses on any requirements that can be traced directly to use cases or business functions and business rules. The goal of this test is to verify proper data acceptance, processing, and retrieval; and the appropriate implementation of business rules.

Gap Analysis Document (GAD)	Formal findings from an analysis comparing existing (As Is) legacy business operations and functionality against future desired (To Be) business operations and ATIMS JMS functionality.
Gap Analysis	The body of work needed to understand the variance between current County (As Is) business requirements and system capabilities vs a desired future state (To Be) including the capabilities of the ATIMS JMS. Scope includes business functionality, interfaces, data migration, security, training, and other aspects of the project.
Interface Control Document (ICD)	Documents the functional and technical requirements of an Interface.
Interface	The programming languages, codes, and messages that software applications use to communicate with each other and to exchange information.
JMS	The ATIMS SaaS InCustody Jail Management System (JMS)
Load Testing	A performance test which subjects the target-of-test to varying workloads to measure and evaluate performance behaviors and ability of the target-of-test to continue to function properly under these different workloads.
Milestone	A milestone represents the completion of one or more deliverables in a particular Track. Milestones mark the completion of incremental steps or parts of the project. A Milestone may be tied to a specific payment and include payment for more than one deliverable
Module	A discrete and identifiable part of the Software performing logically related functions.
Onsite	Activity conducted at County facilities in Sonoma, CA
Performance Testing	Composed of load, stress, and soak testing to ensure the JMS meets response time requirements when deployed to all users and used during peak workloads.
Project Management Plan (PMP)	Is the master formally approved document that defines how the project is executed, monitored, and controlled. The PMP includes baselines and multiple subplans (Risk Plan, Communication Plan, Training Plan, etc.)
QA Log	A log shared by ATIMS and the County to record all software functional and technical issues, their status and resolution.

Regression Testing	Re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change.
Report Testing	Is composed of Component, Function and Regression testing of reports with any feature set that offers a reporting function.

Requirements Traceability Matrix (RTM)	A document that contains and traces the County's RFP and added requirements against ATIMS proposal responses, is cross-referenced to JMS functionality (e.g. modules, screens, reports, and forms) and includes testing and acceptance results.
SaaS	Software as a Service
Scripted Testing	The execution of testing using a pre-determined script or instructions. This testing can be either manual or automated.
Security and Access Control Testing	Focuses on two key areas of security: i) Application-level security including access to the data and business functions ii) System-level security including login into or Remote access to the system
SME	Subject Matter Expert in one or more business or technical domains.
SO	Sonoma County's Sheriff's Office
Software	The ATIMS Jail management system (JMS)
Stability Period	A ninety consecutive (90) day period after Go Live where the JMS operates in a live production environment without Severity Level 1 or Severity Level 2 Errors and satisfactory resolution of Severity 3 and 4 Errors.
Support Turnover Packet	After Go-Live, on transitioning to Customer Support, information on ATIMS Support policies and procedures.
System Testing	End-to-end testing composed of the JMS using test cases used in Functional Testing with migrated data.
Task	An activity or piece of work in the Project Management Plan that may or may not be related to a specific deliverable.
Test Scripts	A series of documented actions, functions, steps or commands for the purpose of execution during quality assurance testing, including system, performance, regression, and user acceptance testing.
TSS	Technology Services and Support (County IT)
User Acceptance Testing (UAT)	Operational testing of the JMS by Sheriff's Office end users to ensure the JMS modules and functions perform to JMS Documentation, specifications, and SOW-DED requirements in real-world scenarios.

Unit Testing	Developer produced tests, confirmed by QA to verify basic operation of the target-of-test requirements.

Updates	"Bug" fixes and other updates, enhancements, upgrades, new version releases, or re-releases of the Software which are made generally available without charge by ATIMS to ATIMS's Clients, except for new applications for which ATIMS charges a separate fee to its Clients.
User	An individual, whether a County employee or contractor, to whom the County has created an account and password, to allow access to the JMS
Work Breakdown Structure (WBS)	A visual, hierarchical, and deliverable oriented deconstruction of a project based on the Phases, Tracks, Deliverables, and Tasks tracked in MS Project.
Workshop/Session	One or more sessions between ATIMS and County resources for the purpose of accomplishing one or more Tasks in this SOW. Most Workshops will be held to conduct analysis, configuration, create and review design specifications, and training. Every Workshop shall be preceded by delivery and review by the County of an agenda. Participants in a Workshop are expected to collaborate to produce a product or result.

Appendix B: Deliverable Summary

Task #	ID #	Deliverable	Type	DED	Updatable
PHASE 1: INCEPTION					
Track 1) Planning					
1.1	1	Kickoff Presentation	Document	No	No
1.2	2	Kickoff	Meeting	YES	No
1.3	3	Discovery & Walkthrough	Activity	No	No
1.4	4	Project Management Plan (PMP)	Document	YES	YES
1.5	5	Project Work Plan (Schedule)	Document	YES	YES
1.6	6	Project Management Artifacts	Document	No	YES
1.7	7	Requirements Traceability Matrix (RTM)	Document	YES	YES
		Milestone 1) Initiation and Planning			
Track 2) Installation					
2.1	8	Base JMS - Installation	Software	No	YES
2.2	9	Base JMS - Documentation	Document	YES	YES
2.3	10	Core Team Training	Training	No	No
		Milestone 2) Installation			
		Stage Gate 1: Planning Complete			
PHASE 2: ELABORATION					
Track 3A) Business Analysis					
3.1	11	Business (Gap) Analysis	Activity	YES	No
3.2	12	GAD - Draft Gap Analysis Document (GAD)	Document	YES	No
3.3	13	GAD - Review Workshop	Meeting	No	No
3.4	14	GAD - Final Gap Analysis Document (GAD)	Document	No	YES
		Milestone 3A) Business Analysis			
Track 3B) Analysis - Modifications					
3.5	15	Modifications - Design Specifications	Document	YES	YES
		Milestone 3B) Analysis - Modifications			
Track 3C) Analysis - Interfaces					
3.6	16	Interfaces - Interface Plan	Document	YES	YES
		Milestone 3C) Analysis - Interfaces			
Track 3D) Analysis - Migration					
3.7	17	Conversion Planning Workshop(s)	Meeting	No	No
3.8	18	Conversion Plan	Document	YES	YES
3.9	19	Data Map	Document	No	YES
		Milestone 3D) Analysis - Migration			
		Stage Gate 2: Requirements Design Complete			
PHASE 3: BUILD					
Track 4) Configuration					
4.1	20	Configuration - User Roles & Security	Software	No	YES
4.2	21	Configuration - System Admin	Software	No	YES
4.3	22	Configuration - Modules (with Workflow)	Software	No	YES
		Milestone 4) Configuration			
Track 5A) Build - Modifications					
5.1	23	Modifications - Development (Test / Fixes)	Software	No	YES
		Milestone 5A) Build - Modifications			
Track 5B) Build - Interfaces					
5.2	24	Interfaces - Interface Control Documents (ICD)	Document	YES	YES

5.3	25	Interfaces - Development & Testing	Software	No	YES
		Milestone 5B) Build - Interfaces			
Track 5C) Build - Migration					
5.4	26	Test Runs (ETL)	Software	No	No
5.5	27	Final Conversion Report	Document	No	No
		Milestone: 5C) Build - Migration			
Track 5D) Build - Forms & Reports					
5.6	28	Forms - Specifications	Document	YES	YES
5.7	29	Forms - Development (Tests)	Software	No	YES
5.8	30	Reports - Specifications	Document	YES	YES
5.9	31	Reports - Development (Tests)	Software	No	YES
		Milestone 5D) Build - Forms & Reports			
		Stage Gate 3: Configuration & Build Complete			
Track 6) Test					
6.1	32	Acceptance Test Plan (ATP)	Document	YES	YES
6.2	33	System Testing	Software	No	YES
6.3	34	Performance Testing	Software	YES	YES
6.4	35	User Acceptance Testing (UAT)	Support	No	YES
6.5	36	Final Test Report	Document	No	YES
		Milestone 6) Test			
		Stage Gate 4: Testing & User Acceptance Complete			
PHASE 4: TRANSITION					
Track 7) Train					
7.1	37	Training Plan	Document	YES	No
7.2	38	Training Documentation	Document	No	YES
7.3	39	Forms - Training	Training	No	No
7.4	40	Reports - Training	Training	No	No
7.6	41	Admin & Technical Training	Training	No	No
7.7	42	Train the Trainer Training	Training	YES	No
7.8	43	End User Training (EUT)	Training	No	No
7.9	44	Final Training Report	Document	No	No
		Milestone 7) Train			
Track 8) Go Live					
8.1	45	Go Live Plan	Document	YES	YES
8.2	46	Go Live Preparation	Activity	No	No
		Stage Gate 5: Cutover Complete			
8.3	47	Go Live Conversion Cutover	Software	No	No
8.4	48	Go Live - On Site Support	Activity	No	No
8.5	49	Transition to Support	Meeting	No	No
		Milestone 8) Cutover			
Track 9) Post Go Live					
9.1	50	Post Go Live Deliverables	Activity	YES	No
9.2	51	Post Implementation Evaluation Report (PIER)	Document	YES	No
Track 10) Close					
10.1	52	Project Close Out	Meeting	No	No
		Milestone 10) Close			

ATTACHMENT 1 - DELIVERABLE EXPECTATION DOCUMENT (TEMPLATE)

This template describes the required contents of a deliverable expectation document.
Work plans that support the activity summary can be attached and may be referenced to support the methodology and schedule summary.

INTRODUCTION

A brief overview defining the purpose of the deliverable and how it fits within the overall completion of the project. Indicate if there are pre-requisite tasks and subsequent tasks.

DELIVERABLE DESCRIPTION

Describe the deliverable's objectives and scope. Discuss the level of detail to be provided such as "will describe the rationale for design decisions, will provide a textual summary of the design with detailed design pseudocode in the appendices, will include database schema diagrams and database table relationships, field sizes and descriptions, and indices and keys".

METHODOLOGY FOR CREATING THE DELIVERABLE

Provide a brief explanation of the tasks, activities and methods to be used to develop the deliverable. If appropriate, include a process flow diagram. Do not duplicate methodologies described elsewhere (e.g., if the design methodology was described in detail in the proposal and project management plan, reference the appropriate document section). Indicate if there are any assumptions or constraints on the development of the deliverable.

TABLE OF CONTENTS

List the table of contents or outline of the document. Discuss the content of each major section. Where appropriate or as requested by the project, provide a sample of this document from other engagements/projects or sample content, level of detail and format of key sections.
Section 1 – Introduction -This section will provide a high-level overview of the deliverable, its scope and purpose.

Section 2 –

Section 3 –

Appendix A –

DELIVERABLE REQUIREMENTS

List the specific requirements for this deliverable from the Request for Proposal, Statement of Work, and/or contract. List the specific source of the requirement, including document name, document date/version, paragraph or page number, and requirement number (from the Requirements Traceability Matrix/Database).]

Table 1. Deliverable Requirements (Example)

REQ #	REQUIREMENT DESCRIPTION	SOURCE OF THE REQ	COMMENT

DELIVERABLE FORMAT

List any required templates, diagrams, tables or specific content required for this deliverable. For instance, in design and test deliverables, an updated requirements traceability matrix should be included in the final deliverable.
Indicate the format of the document and any associated diagrams, spreadsheets (e.g., MS Word, MS Visio, MS Project, etc.)

DELIVERABLE ACCEPTANCE CRITERIA

[List the specific acceptance criteria for the deliverable. The first criteria should always be "were the requirements met". The criteria should be specific to the deliverable and indicate key needs of the project (e.g., must include detailed description of database sizing, growth considerations, performance considerations, and de-/normalization considerations).
Other general review criteria (which are primarily the same for all deliverables) may be referenced or attached. The following are the minimum acceptance criteria.]

- *Were all requirements (above) met?*
- *Did the deliverable comply with the stated format above)?*
- *Is the deliverable consistent with other deliverables already approved?*
- *Did the deliverable meet the general review criteria (e.g., pages numbered, free of formatting and spelling errors, clearly written, no incomplete sections, etc.)?*

DELIVERABLE SCHEDULE

Key Deliverable Dates

List the key activities and due dates in the preparation and review of this deliverable. If appropriate, list key meetings, walkthroughs, inspections and reviews. These tasks should be consistent with the activities and dates in the workplan and contractual timeframes regarding deliverable delivery, review and approval/rejection.
Include time for state review of the deliverable and ATIMS incorporation of comments. Indicate if any activities/dates are on the critical path or have significant dependencies. The following is a sample.

Table 2. Key Deliverable Dates (Example)

KEY ACTIVITY	DUE DATE	COMMENT
DED Approval	xx/xx/20xx*	
Internal Walkthrough with Project		
Draft Deliverable Submitted		
State Review of Draft		Minimum of 1 week
Walkthrough of Draft with Stakeholders		
Deadline for Comments on Draft		
ATIMS Incorporation of Comments		
Final Deliverable Submitted		
State Review of Final		Minimum of 1 week
Deliverable Approval		
ATIMS Incorporation of Final Comments (if necessary)		

*Critical Date

Schedule for Deliverable Updates

[If the deliverable is expected to be updated on a periodic basis, list the proposed schedule of updates and tentative time frames. Dates may be either "hard dates" (e.g., May 5, 2022) or "soft dates" (30 days prior to System Test). If appropriate, reference the appropriate RFP/SOW requirement for the update.]

Table 3. Deliverables Update Schedule (Example)

REASON FOR DELIVERABLE UPDATE	SOW REFERENCE	DATE DUE	COMMENT
Incorporate any changes from Code/Unit Test phase	[Reference, as used in SOW; i.e., paragraph #, or unique reference]		
Incorporate any changes from the Integration and System Test phase	SOW para 3.2		
Incorporate any changes from the Acceptance Test phase			
Incorporate any changes from the Implementation phase			

REQUIRED COUNTY RESOURCES

List the specific resources involved in the deliverable preparation and review. Estimate the amount of time required from each County resource, particularly for any sponsor, user, or stakeholder staff involved. If appropriate, list the specific skill or knowledge required, such as knowledge of case management policy or experience with current system's reports. It is not necessary to list all ATIMS staff involved in the preparation, only the key County staff or required skills. This list is not intended to replace the workplan resources, but to identify specific individuals/skills needed to ensure successful completion of the deliverable.

Table 4. Required Resources (Example)

ROLE	NAME(S)	RESPONSIBILITIES	ESTIMATED NEED
Deliverable Approver			5 days
Deliverable Reviewers			7 days
Subject Matter Experts			10 days
Policy Representative			10 days
IV&V			5 days

SIGNATURE BLOCK (County / ATIMS)

Attachment 2: Deliverable Notice (Example)

NOTICE OF DELIVERABLE DELIVERY

Agency Name: County of Sonoma

Project Sponsor:

To: _____

The following deliverable has delivered to Sonoma County per the Statement of Work and any applicable Delivery Expectation Document requirements.

Deliverable #: _____

Deliverable Title: _____

Deliverable Date: _____

Delivery Method: _____

Comments:

_____ _____

ATIMS Project Manager Signature Date

Attachment 3: Acceptance Notice (Example)

COUNTY ACCEPTANCE OF DELIVERABLE

Agency Name: County of Sonoma Project

Sponsor:

To: _____

The following deliverable has been received and reviewed by Sonoma County

Deliverable #: _____

Deliverable Title: _____

This deliverable:

_____ Is accepted as written _____ Requires changes as indicated

Comments:

_____ _____

Project Manager Signature Date

_____ _____

Project Sponsor Signature Date

Attachment 4: Change Request Form (Example)

JMS PROJECT CHANGE REQUEST

Request Number: _____

Request Date: _____

Requested By: _____

Request Title: _____

Description of Change Request:

Justification for Change Request:

Impact of Change:

Scope: _____

Cost: _____

Timeline:_____

_____ _____

Project Manager Signature Date

_____ _____

Project Sponsor Signature Date

TECHNOLOGY
SERVICES AND SOLUTIONS

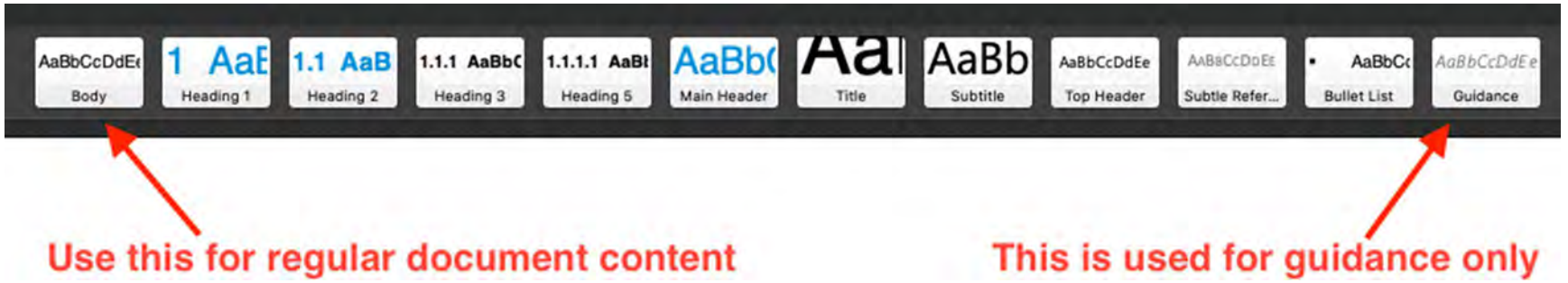
Optional Insert image (from TSS image library)

Integration Design Document Template

<Integration Name>

Table of Contents

<This template contains various guidance text under the various document sections that will be displayed in gray and italics between <> brackets using the "Guidance" Word document style used for styling this paragraph. This text is meant to identify owners for each of the sections and provide guidance on what content to include under each section. As you work your way through the document please read and follow the guidance then make sure to delete guidance text across the document (including this paragraph and screenshot below) before the document is finalized. Actual content under the various sections should always use the "Body" style formatting.>



1 Introduction

<This section should be completed by the Business Analyst and validated by the Integration Architect and Data Architect.>

<This section should provide a high-level overview of the integration, including things such as:

- *Description of what integration will be used for*
- *Brief description of the scope of the integration>*

1.1 Purpose

<Provide purpose for the integration being built. Why is the integration needed?>

<Select criticality of the integration using the following table and provide explanation of why.>

Check the appropriate box	Criticality	Description
X	C (Critical)	Business cannot operate
	H (High)	Business can operate but heavy manual requirement
	M (Medium)	Business can operate but not optimization
	L (Low)	Business minimally improved

1.2 Business Benefits

<Use the below table to provide an overview of the business value / benefits achieved by the integration and how it will help the business.>

#	Name	Description
1	<Add short name for benefit #1>	< Include a detailed description of the benefits that will be achieved once the integration is built. Examples should include time saved on certain tasks, cost savings, quality improvements, Return on Investment, etc.>
2		
3		

1.3 Integration Parties

1.3.1 Parties Involved in Integration

<Use the below table to provide relevant details for all parties involved in this integration along with a description of how involved with the integration (e.g., sending agency, receiving agency, bidirectional integration partner, subscriber, publisher, integration facilitator (used for integration engines such as the Information Sharing Environment (ISE)), etc.) and primary contact information.>

Name	Involved System Name	Description of Involvement	Primary Contact Info
<Enter name of the various parties involved in the integration, including County agencies, third party vendors, other involved parties, etc.>	<Enter name of the system(s) used by the party for integration>	<Enter description of the party's involvement in the integration here>	<Enter name and contact info for the primary contact associated with the party>

1.3.2 Integration Stakeholders

<Use the below table to provide relevant details for all stakeholder parties involved in this integration along with role (e.g., data owner, business owner, project sponsors, etc.) and contact information.>

Name	Role	Contact Email	Contact Phone
<Enter name of the various stakeholder parties involved in the integration, including representatives of County agencies, third	<Enter description of the party role(s) and duties here>	<Enter email associated with the party main contact(s)>	<Enter phone number associated with the party main contact(s)>

party vendors, other stakeholders, etc.>			

1.4 Integration Development Roles

<Use the below table to list the names of individuals performing the various key roles associated with the development of this integration.>

Role	Name	Description of Duties
Product Owner	<Add name here>	Responsible for leading all project activities associated to this integration effort
Business Analyst	<Add name here>	Responsible for providing functional expertise on the systems being integrated and the overall scope of the integration
Integration Architect	<Add name here>	Responsible for providing architectural-level design approach and guidance for developing the data exchanges and bridging the gap between the business and technical teams as needed
Data Architect	<Add name here>	Responsible for specifying the detailed data field specifications and mappings required to meet the business requirements
Security Engineer	<Add name here>	Responsible for ensuring best practices for the security of the integration and providing all security requirements needed in order to deploy the integration including field-level security when applicable.

Integration Engineer	<Add name here>	Responsible for developing the core code of the integration according to the specifications outlined by the business analyst, data architect, and integration engineer team
Test Engineer	<Add name here>	Responsible for the testing of the integration functionality and completion of test results

1.5 Out of Scope Items

<Provide a list of items that will be out of scope for this integration (e.g., cleaning up and backing up data on the Court Odyssey system). This will help steer conversations and set expectations of all involved parities of what the integration will or will not include up front which will impact the rest of the business analysis and technical design and development activities. Out of scope items might need to be revised once deeper analysis is performed and new information is gained but it needs to be updated and agreed upon with all parties before the integration documentation is finalized.>

2 Business Overview

<This section should be completed by the Business Analyst and validated by the Integration Architect and Data Architect >

<Provide overview of the end-to-end business processes related to this integration. Include a brief bigger picture business process context related to this integration to orient the reader to how this integration fits within the big picture. Detailed of business processes not part of this integration should not be included here.>

2.1 Actors

<Use the below table to provide a high-level description of the actors involved in this integration which will be referenced on the business flow diagrams in the following section.>

Actor	Actor Role Description	Comments

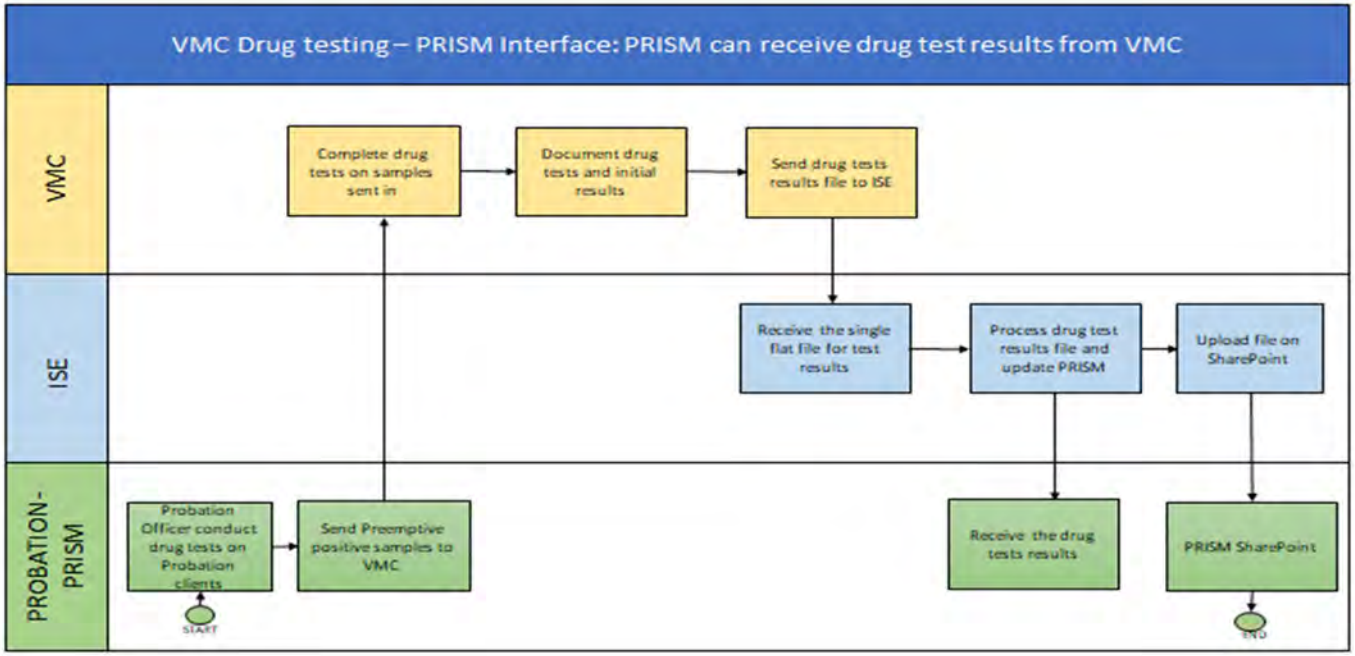
<Enter name of the actors for the specific use case here>	<Enter description of the role/group here>	<Enter comments here>

2.2 Current Business Process

2.2.1 Business Flow Diagram

<Include a diagram showing the current business process flow of the integration, including all involved actors. The diagram should clearly illustrate the flow of each business process and how the various actors interact with each other end-to-end. The diagram should be created using basic flowchart design with arrows pointing to the next logical flow of information and boxes describing the action taken by the respective actors each within their swim lane.>

<Sample Diagram>



2.2.2 Business Narrative

<Provide overview of the current end-to-end process related to the integration for how the business operates before the integration is built.>
<Sample narrative points which need to be further elaborated:

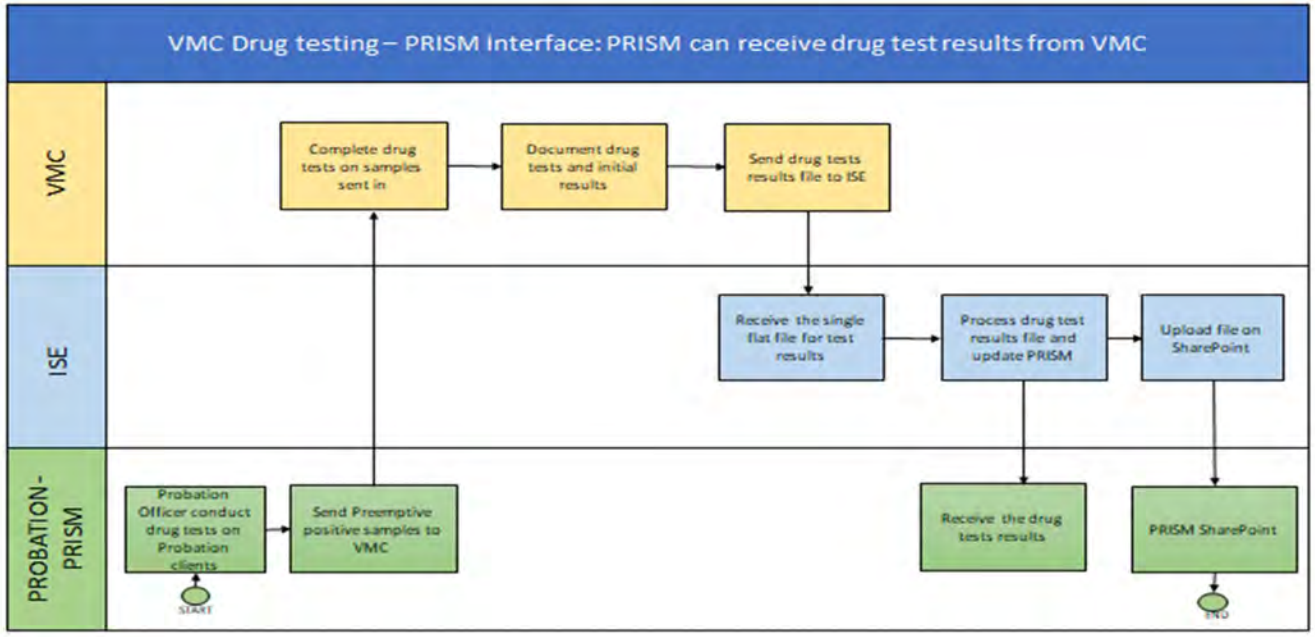
- *Currently, CJIC data is being sent to Court system*
- *The current process has 11 integration points that are used to send data*
- *Out of the 11 integration points, 4 are currently completely manual using data entry by Court clerks*
- *etc.>*

2.3 Future Business Process

2.3.1 Business Flow Diagram

<Include a diagram showing the future business process flow of the integration, including all involved actors. The diagram should clearly illustrate the flow of each business process and how the various actors end-to-end interactions with each other will be changed after the integration is built and deployed. The diagram should be created using basic flowchart design with arrows pointing to the next logical flow of information and boxes describing the action taken by the respective actors each within their swim lane.>

<Sample Diagram>



2.3.2 Business Narrative

<Provide overview of the future end-to-end process using bullet point format for how the business will operate after the integration is built and deployed. Future processes should be related to integration only.>

<Sample narrative points which need to be further elaborated:

- *The integration will automate the 4 manual integration points*
- *Data will then be picked up by a scheduler and sent to the Court system through a queue>*

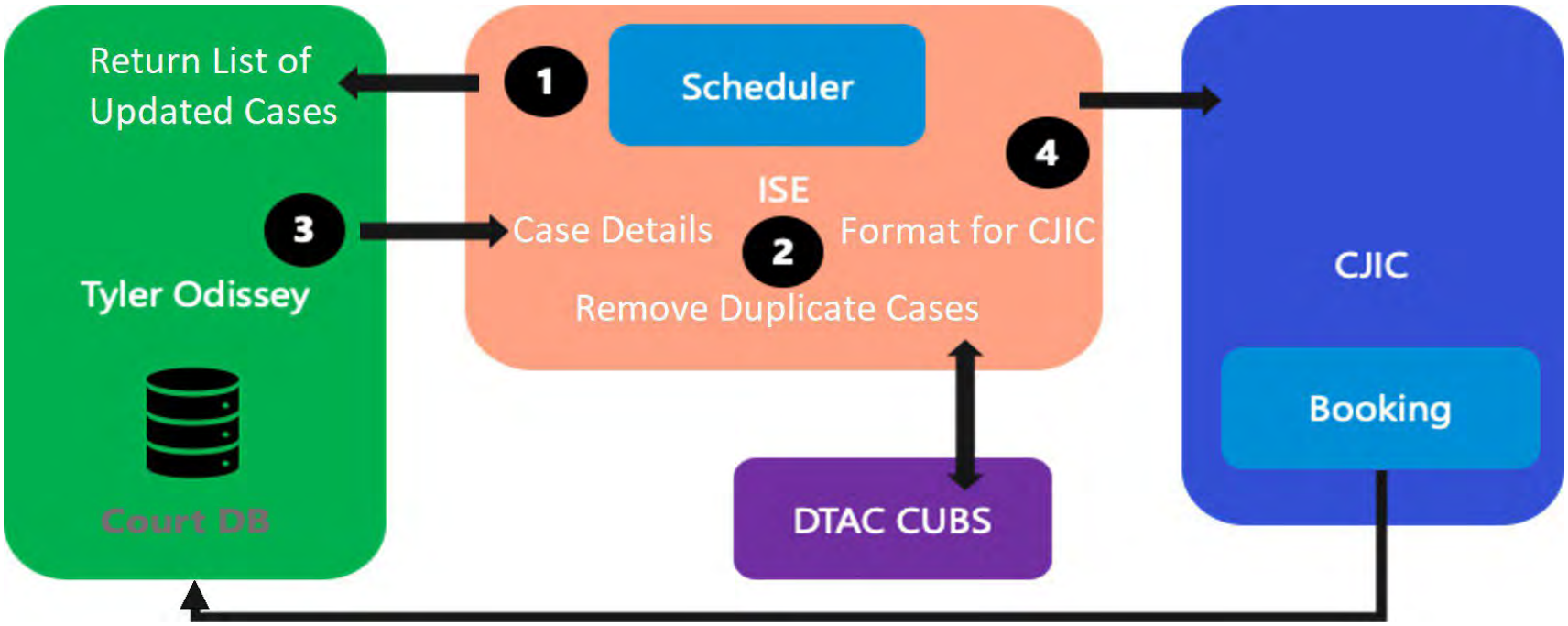
3 Integration Overview

<This section should be completed by the Business Analyst and validated by the Integration Architect and Data Architect.>

3.1 Integration High-Level Diagram

<Include a diagram that shows sequence of how the information will flow through the integration being built at a high-level, including source and destination systems (e.g., check for updated cases in Count Tyler Odyssey as the data source system, eliminate duplicate cases, get case details for each cases, format the data for CJIC and send it to CJIC as the target system, get Booking data from CJIC as the source system and sent it to Count Tyler Odyssey as the target system, etc.)>

<Sample Diagram>



3.2 Integration Process Description

<Use the below table to describe the various steps that are required to enable this integration as shown in the high-level integration diagram in section 3.1.>

#	Process Step	Comments
1	Checks on updated cases in Tyler Odyssey every few minutes	
2	Eliminate duplicate cases	

3	Get case detail data from Tyler Odyssey for each updated case	
4	Format the data in CJIC format and sent to CJIC	
5	Send Booking data from CJIC to Tyler Odyssey every X for booking that are XYZ, etc.	

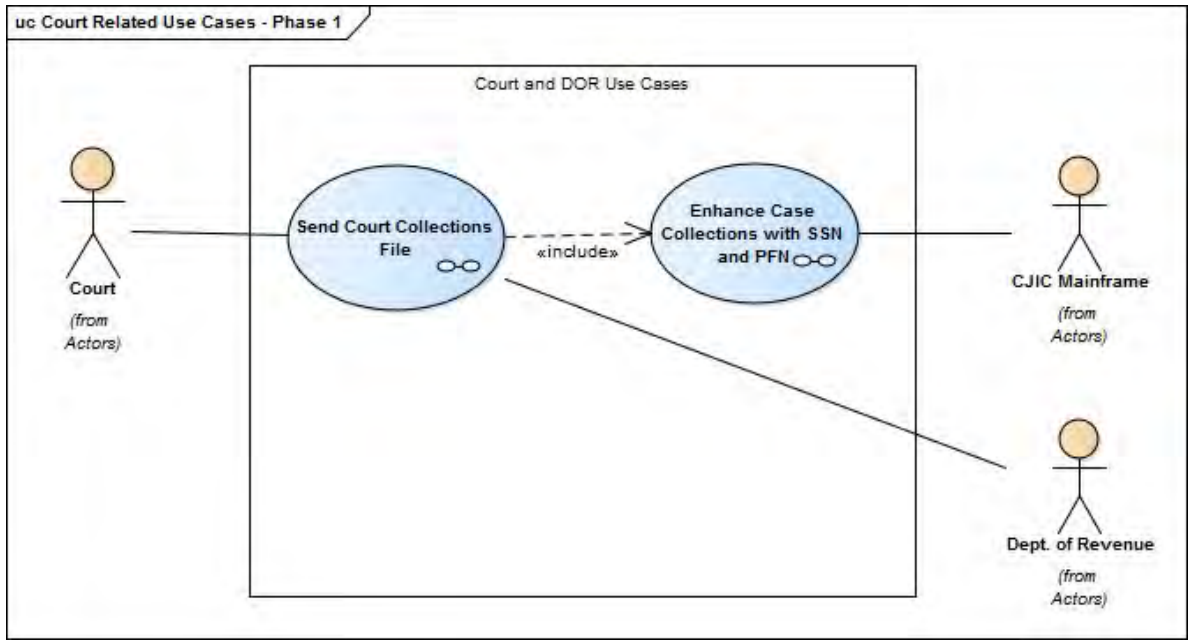
3.3 Use Cases

<Provide a summary of the use cases for this full integration (e.g., Court Clerk will send a court collection file and the Department of Revenue will receive the file from the integration).>

3.3.1 Use Cases Overview Diagram

<Include a diagram that shows the summary of all use cases related to this integration.>

<Sample Diagram>



3.3.2 Use Cases List Overview

<Use the below table to explain in detail each use case and create a diagram to showcase the end-to-end process for use cases.>

#	Name	Sender	Receiver	Frequency	Comments
1	<Enter name of the use case>	<Enter the name for the person acting as the sender for this specific use case>	<Enter the name for the person acting as the receiver for this specific use case>	<Enter the frequency for the specific use case related to the business>	<Enter comments here>
2					
3					

3.3.3 Use Case #1

3.3.3.1 Description

<Provide a brief description of this specific use case and how it fits into the full integration.>

#	Pre-Conditions	Post-Conditions	Comments
1	<List any conditions that need to occur before the integration executes>	<List any expected conditions after the integration executes>	
2			
3			

3.3.3.2 Narratives

<Provide a narrative of this specific use case, including the actors and actions against the systems.>

3.3.3.3 Actors

<Use the below table to list the actors that take actions related to this specific use case.>

Actor	Actions Taken	Comments
<Enter name of the actors for the specific use case here>	<Explain how they engage in the activities describe in the use case above>	<Enter comments here>

3.3.3.4 Business Rules

<Provide all business rules associated with this specific use case. What are the rules needed for the use case to be considered completed?>

BR #	Business Rule	Comments
1	Business rule #1	
2	Business rule #2	
3		

3.3.3.5 Assumptions

<Provide all assumptions associated with this specific use case.>

3.3.3.6 Security Considerations

<Add any security considerations related to this specific use case and associated fields here. For example, ensure that sensitive data (e.g., data related to CJIS, HIPPA, PII, PCI, etc.) is protected and cannot be viewed by all users unless authorized with the proper group-level credentials, etc.>

3.3.3.7 Entity List (List of fields)

<Use the below table to list all fields needed by this specific use case.>

#	Entity Display Name	Field Display Name	Data Type	Min Value	Max Value	Default Value	Required?	Comments
1	<Enter display name for the entity here>	<Enter the name for how the field is	<Enter the data type for the field here>					

		displayed here>						
2	Client	First Name	Text					
3	Court	Case Status	Option Set					

3.3.4 Use Case #X

<Please copy and paste section 3.3.3 (including sub-headers) for additional use cases as needed (e.g., use case #2 would become section 3.3.4, etc.). The table under section 3.3.2 should be updated at the end to list all use cases added to this document.>

4 Integration Technical Approach

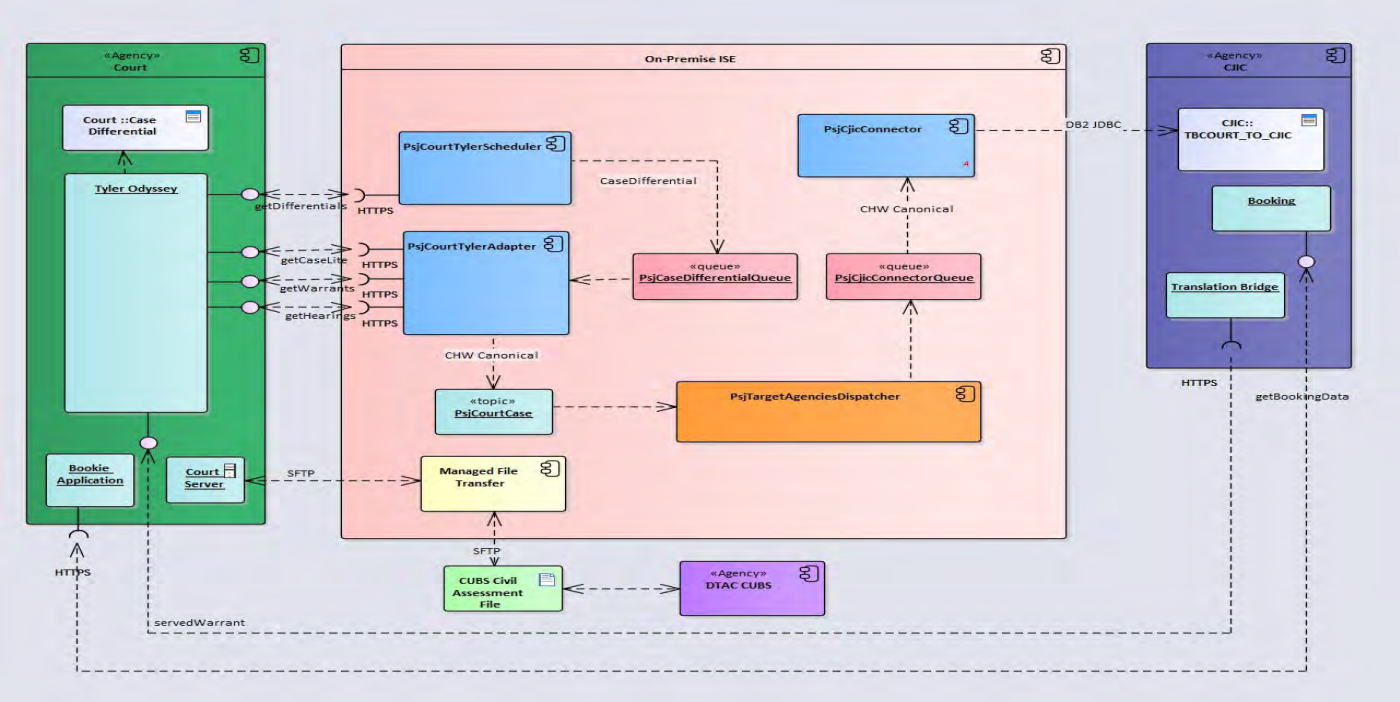
<This section should be completed by the Data Architect and Integration Engineer using guidance from the Integration Architect and with input from the Business Analyst.>

<Describe a summary of the approach for building the integration based on the details elaborated in following sections.>

4.1 Integration Overview Diagram

<Include a detailed technical diagram for the integration including specifics about the methods called by the various systems and the various APIs being leveraged by the end-to-end integration, connectors being used, etc. This diagram should significantly expand on the high-level diagram provided in Section 3.1. providing the technical design specifics.>

<Sample Diagram>



4.2 Integration Approach

<Use the below table to list details on how the integration picture in the diagram above will work and how it will process the information end-to-end (e.g., steps to perform before message is sent to target, used connector / adapters, schedulers used to initiate actions, etc.)>

<Sample Steps>

#	Process Steps	Comments
1	Describe how the scheduler is triggered and how it sends the CaseDifferential information to the DifferentialQueue	<Enter comments>

2	Describe how the messages are processed and what protocols are used to process the information. How is the data being sent to the adapter before it goes to the Tyler Odyssey Court system?	
3	How does ISE send data to the Court Tyler Odyssey system? Which APIs are being called and how is the data sent back to ISE from the Odyssey Court system? <Continue describing the technical details of each process until completion of the integration.>	

4.3 Integration Data Exchange List

<Use the below table to provide a comprehensive list of data exchanges for the integration being built. This list should include any APIs, connectors, adapters, file exchanges, and other data exchange points required by the end-to-end integration shown in the diagram in section 4.1>

#	Data Exchange Name	Data Exchange Description	Data Exchange Type	Frequency	Data Exchange Owner	Use Case Mapping	Comments
1	<Enter data exchange name>	<Enter description of functionality of the data exchange>	<Enter the type of data exchange (e.g., REST API, FTP, etc.)>	<Enter frequency for the data exchange (e.g., near real-time, hourly, daily,	<Enter the name for the owner of the data exchange>	<Enter the specific use cases that this data exchange maps to>	<Enter comments>

				monthly, etc.)>			
2							
3							

4.4 Data Exchange #1

<Reference the SCC PSJ best practices and technical guidelines relevant to this specific data exchange type (e.g., REST, SOAP, flat file, etc.)>

4.4.1 Overview

<Provide a brief overview of this specific data exchange.>

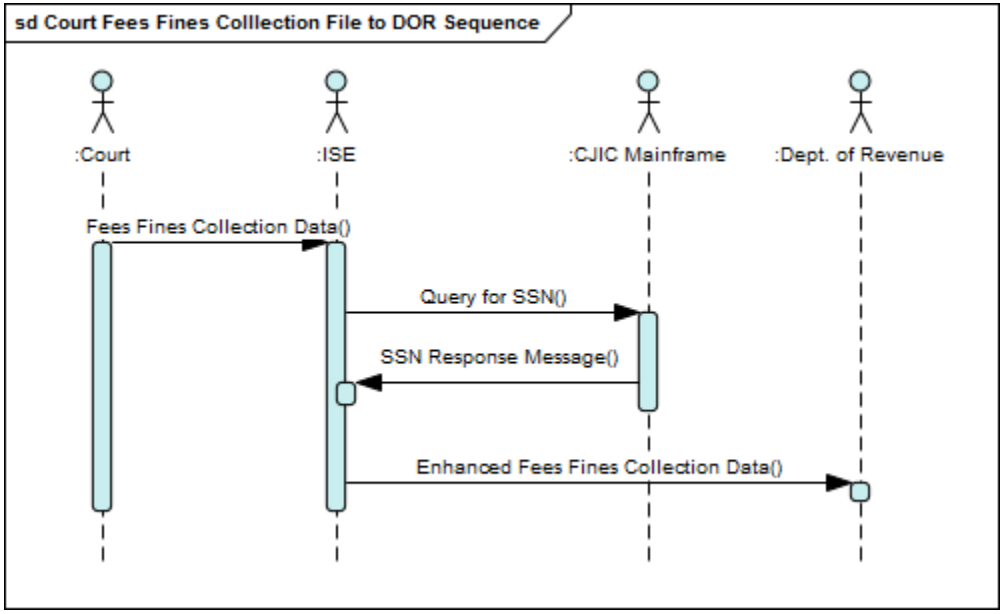
4.4.2 Actors

Actor	Actor Role Description	Comments
<Enter name of the actors being described in the data exchange diagram of the following section>	<Enter description of the roles played by the actor in the data exchange diagram of the following section>	<Enter comments here>

4.4.3 Sequence Diagram

<Include a detailed diagram that shows the sequence and the various components of this specific data exchange as they interact with each other. The diagram should include numbering to show the sequence of events and the methods called as the data exchange is being executed end-to-end.>

<Samples Diagram>



4.4.4 Steps

<Use the below table to provide details on each method used by this specific data exchange and any associated query and response parameters. Please make sure to include description of what the method does so that it can be potentially leveraged by other developers or other systems in the future for other integrations.>

<Samples Steps>

#	Step / Method Name	Query Parameters	Response Parameters	Description of Data exchange Functionality

1	<Enter step / method name>	<Enter expected parameters here for the data exchange query>	<Enter expected parameters here for the data exchange response>	<Enter description of the data exchange>
2	Query for SSN()	Var personIdentifier;	Var personIdentifier;	The method queries the system for Social Security Number based on the parameter passed to the method. It passes a unique identifier to the target system.
3	SSN Response Message()	Var SSNText;	Var SSNText;	The method queries the database for SSN based on the parameter passed by the Query for SSN() method; It returns a string with the Social Security Number.

4.4.5 Data Workbook

<Use the attached data workbook to provide detailed field specifications, data mapping, and associated reference data required for this specific data exchange. The workbook also contains different columns of mapping types (e.g., XML, fixed-file) and you should only filled the columns that apply to the type of mapping specific to this data exchange type (e.g., if XML-based, you do not need to use the "Starting Position" column, etc.).>

4.4.5.1 Code Specifications

<If there are any active developed data exchange specifications (e.g., OpenAPI, WSDL / XSD, etc.), insert a link to the active documentation below and ensure that the Data Workbook details are updated to reflect the actual code field specifications.>

4.4.6 Privacy & Security Requirements

<Use the below table to list any security integration-level requirements (e.g., sensitive data handling, access logging, security logging, etc.)>

<Samples requirements>

#	Requirement Name	Requirement Description
1	Security Logging	Ensure that data exchange has a way to track the users that modify the data and that started the data exchange process
2	Contains Sensitive Information	Ensure that sensitive data (e.g., data related to CJIS, HIPPA, PII, PCI, etc.) is protected and cannot be viewed by all users unless authorized with the proper group-level credentials
3		

4.4.7 Exception Handling

<Provide an explanation of the approach for handling exceptions covering both data / business exceptions that require business users intervention to address and technical exceptions along with the approach to address these two category of exceptions when they occur. Use the below table to provide an overview of the exception handling process and any additional details on how the data exchange will behave when errors occur, including exception processing. Include any error codes and error messages that will be expected from the data exchange.>

#	Exception Response Code	Exception Description	Resolution Actions
1	<Enter any specific error codes that may be thrown by the data exchange.>	<Enter description for the specific error code.>	<Enter any actions that can be taken to resolve this specific exception code.>
2			
3			

4.4.8 Samples Data

<Use the below table to attach / embed any samples of the actual integration data messages, files, etc.>

#	Name of Sample File	Description of File
1	<attach sample file here>	<Enter description of sample file here>
2		
3		

4.5 Data exchange #X

<Please copy and paste section 4.4 for additional data exchanges as needed (e.g., Integration #2 would become Section 4.5, etc.). The table under section 4.3 should be updated at the end to list all data exchanges.>

5 Integration Testing

<This section should be completed by the Test Engineer and Business Analyst with input from the Integration Engineer for the code test coverage section and validated for quality and comprehensiveness by the Integration Architect.>

5.1 Testing Approach

<Provide the approach that will be used to test the integration as it moves through the development lifecycle (e.g., level of use of automated test tools for the various test types, test script repositories used, test result evaluation and approval process, plan for validating target system(s) data integrity after integration is executed, etc.)>

5.2 Code Test Coverage

<Provide details on approach and plan for code test coverage.>

5.3 Unit Test Scripts

<Use the below table to provide unit test scripts and associated result details.>

Test Scenarios			
#	Test Script	Test Status	Expected Result
1	<Enter test script name here>	<Enter status of test script here (e.g., pass/fail)	<Enter expected results here for the specific test script
2	Is a deputy able to enter inmate Demographics and inmate Identifier data? Is a mugshot photo displayed once the PFN and/or CEN record is saved in IRIS? Does a photo appear within 1.5 seconds? Validate that all added and/or updated data events for Inmate Demographics are passed to the ISE. Validate that all added and/or updated data events for Inmate Identifiers are passed to the ISE.		
3			

5.4 System Test Scripts

<Use the below table to provide system test scripts and associated result details.>

Test Scenarios			
#	Test Script	Test Status	Expected Result
1	<Enter test script name here>	<Enter status of test script here (e.g., pass/fail)	<Enter expected results here for the specific test script
2	Is a deputy able to enter inmate Demographics and inmate Identifier data? Is a mugshot photo displayed once the PFN and/or CEN record is saved in IRIS? Does a photo appear within 1.5 seconds? Validate that all added and/or updated data events for Inmate Demographics are passed to the ISE. Validate that all added and/or updated data events for Inmate Identifiers are passed to the ISE.		
3			

5.5 User Acceptance Test Scripts

<Use the below table to provide user acceptance test scripts and associated result details.>

Test Scenarios

#	Test Script	Test Status	Expected Result
1	<Enter test script name here>	<Enter status of test script here (e.g., pass/fail)	<Enter expected results here for the specific test script
2	Is a deputy able to enter inmate Demographics and inmate Identifier data? Is a mugshot photo displayed once the PFN and/or CEN record is saved in IRIS? Does a photo appear within 1.5 seconds? Validate that all added and/or updated data events for Inmate Demographics are passed to the ISE. Validate that all added and/or updated data events for Inmate Identifiers are passed to the ISE.		
3			

5.6 Performance Test Scripts

<Use the below table to provide performance and load test scripts and associated result details.>

Test Scenarios			
#	Test Script	Test Status	Expected Result

1	<Enter test script name here>	<Enter status of test script here (e.g., pass/fail)	<Enter expected results here for the specific test script
2	Is a deputy able to enter inmate Demographics and inmate Identifier data? Is a mugshot photo displayed once the PFN and/or CEN record is saved in IRIS? Does a photo appear within 1.5 seconds? Validate that all added and/or updated data events for Inmate Demographics are passed to the ISE. Validate that all added and/or updated data events for Inmate Identifiers are passed to the ISE.		
3			

6 Deployment

<This section should be completed by the Integration Engineer and validated by the Integration Architect.>

<Provide a description of the approach to implementing the integration once it's developed, including the following:

- *How is this integration being managed in the deployment pipeline?*
- *Which environments is this being deployed to?*
- *What is the process to approve the deployments?*

- *What is the Include a list of requirements for deployment (e.g., infrastructure, network setup, list of environments>*

6.1 List of Environments

<Use the below table to provide a list of environments that will be used throughout the development lifecycle of the integration and any associated infrastructure requirements.>

#	Environment Name	Environment Description
1	<Enter environment name such as Dev, Test, etc. >	<Enter description of use and associated environment infrastructure specifications>
2		
3		

6.2 Deployment Considerations

<Provide any requirements for the deployments (e.g., required security configurations or firewall updates, new roles to be created or permissions to be configured, etc.). This section should also include the process for approval of moving code between environments.>

6.3 Deployment Pipeline

<Provide approach and details around the toolchain and pipeline being leveraged for any deployments (e.g., specifics on how Azure DevOps be leveraged to deploy the integration, etc.)>

6.4 Integration Training

<Provide the approach and plan to train up the group of users (business and technical) that will be using the integration once it's deployed to Production (e.g., who will be developing the training material, who will perform the training, where will the training materials be stored for future use and onboarding, etc.)>

6.5 Contingency Planning

<Provide workarounds / procedures if the integration is not available and how the business should behave if the integration is not available. Please make sure to provide links to any manual processes or worksheets that will be needed for this or add to the appendix section at the end of this document.>

7 Maintenance

<This section should be completed by the Business Analyst and Integration Engineer and validated by the Integration Architect.>

7.1 Support Team Structure

<Use the below table to list the various roles and individuals that will be responsible for the support activities of this integration post Go-Live.>

Support Role	Name	Description of Duties	Contact Info (Email/Phone)
<Enter support role name>	<Add name here>	<Enter description of responsibilities>	
Help Desk Agent	<Add name here>	Responsible for leading first level of support when issues come up	
Integration Support Engineer	<Add name here>	Responsible for resolving any technical issues with the data exchange	

Integration Monitoring Lead	<Add name here>	Responsible for ensuring integration is properly monitored and any parties are notified in a timely fashion once issues occur	

7.2 Operations

<Provide a list of activities required for operations of this integration (e.g., log file maintenance, storage management, backups, etc.)>

7.3 Monitoring

<Provide description of how the various data exchanges under this integration will be monitored (e.g., what specific systems / servers will be monitored, how will 24/7 monitoring be met, required notifications when certain thresholds are breached, escalation paths for different types of notifications, etc.)>

7.4 Issue Resolution

<Provide details on process to handle the operations and monitoring related issues for this integration (e.g., flow diagram for how support works including monitoring team notifying help desk agents and opening tickets for issue resolutions from the Integration Engineers, instructions for when / how to re-execute a specific data exchange to resolve an issue, etc.)>

7.5 Enhancement Considerations

<Provide the process to further enhance the integration once it's been deployed to production including the process to initiate and implement changes to the integration.>

7.6 Integration Versioning

<Provide a description of the versioning approach being used for the integration (e.g., how versioning will be managed when an data exchange is updated post Go-live, how changes are approved and deployed, one or multiple concurrent data exchange versions, related Unified Resource Identified (URI) path management, etc.>

7.7 Reports Considerations

<Provide details on whether this integration requires any specific reporting requirements and if so, describe the type of reports and associated frequency.>

8 Issue Tracking

<This section should be completed and maintained by the Project Manager, Business Analyst and the Integration Engineer with input from all team members.>

<Use the below table to list all issues identified during design and development of the integration>

#	Issue Description	Resolution	Date Resolved

9 Abbreviations

<This section should be completed and maintained by the Business Analyst and Integration Engineer with input from all team members.>

<Use the below table to list all abbreviations referenced throughout this document to ensure that reads that might not be aware of the related acronyms understand what they are related to.>

Term	Description

10 Revision History

<Samples Entries>

Revision #	Date	Revised By	Description
1.0	12/10/2020	John Doe	Initial Draft
1.1	1/5/2021	Jane Doe	Added the integration specifications sub-sections
1.2	1/11/2021	John Doe	Updated the integration mapping table to include additional columns to capture schema and field names
1.3	1/13/2021	Jane Doe	Updated document template to match latest SCC template

11 Appendix

<Include any additional appendix information creating multiple sections using alphabetical order as needed (e.g., Appendix A, Appendix B, etc.)>

Exhibit K
ATIMS InCustody Jail Management System (JMS) Cloud-Solution Service Level Agreement (SLA) & Support & Maintenance Agreement (“Support Agreement”)

Contents

1.0 Definitions

Unless the context otherwise requires, the following terms when used in this SLA & Support & Maintenance Agreement ("Support Agreement") shall have the following meanings ascribed to them:

1. "**Agency Support Contact**" means each County employee authorized by County to submit Support Services requests for ATIMS JMS and Cloud Hosting Services on County's behalf. Each authorized contact will be placed by County on the Authorized User List.
2. "**Agency JMS Administrator**" means each County employee designated by County to serve as technical administrator of the JMS and Cloud Hosting Services on County's behalf. Each Administrator User must complete training and qualification requirements reasonably required by ATIMS.
3. "**Client**" means the County of Sonoma, California.
4. "**Client Content**" means all data and materials provided by Client to ATIMS for use in connection with the JMS and Cloud Hosting Services, including, without limitation, Client applications, data files, and graphics. County Data, as defined in the Agreement, shall also include Client Content.
5. "**Cloud Hosting/ Hosted Environment**" means the Amazon Web Services (AWS) gov cloud and CJIS compliant infrastructure upon which the ATIMS JMS Software is installed in multiple County environments (e.g., Production, Test, Training, Development, Reporting) and operated for the County, including support and maintenance services related to the Cloud Hosting.
6. "**Correction/Correct**" means the use of industry standard efforts by ATIMS to resolve/fix an Incident.
7. "**County**" means the County of Sonoma, California.
8. "**Documentation**" means the user guides/manuals, templates, specifications, workbooks, online help, release notes, training materials and other instructional materials provided or made available by ATIMS to Client regarding the use or operation of the JMS and Cloud Hosting Services.
9. "**Embedded Programs**" means any 3rd party software, modules, products, interfaces, data files and/or other files and programs provided by ATIMS as part of, or in connection with, its JMS Software where ATIMS is the licensee.
10. "**Error**" means an error/malfunction bug in the JMS, which degrades the JMS or the Client's use of the JMS and which is reported to ATIMS as an Incident.
11. "**Fees**" means the Software Subscription Fees, the annual Maintenance and Support Fees and any Additional Services Fees, set forth in Exhibit B: Payment and Fee Schedule.
12. "**Incident/Issue**" means Software or Solution is not performing in accordance with the Documentation or Agreement requirements.
13. "**JMS**" means the ATIMS SaaS InCustody Jail Management System (JMS), provided by ATIMS to the County under the terms of the Agreement between County and ATIMS for a JMS ("Agreement").

14. "**Maintenance Releases**" means any patches, "bug" fixes, updates, upgrades or re-releases of the Software, which are related to specific Software and/or the Cloud Hosted Environment.
15. "**Platform**" "Web-based datacenter that hosts server and related hardware providing on demand remote access to computing services, including, databases, application software, and analytics."
16. "**Professional Services**" means excluding the Support Services, all technical and non-technical services performed or delivered by ATIMS under this Support Agreement, including, without limitation, training and education services. Unless otherwise specified or agreed to by the parties, Other Services will be provided on a time and material (T&M) basis at such times or during such periods, and at rates noted in this Support Agreement. All Other Services will be provided on a non-work for hire basis.
17. "**Software**" means the object code version of the ATIMS JMS described in the SOW and otherwise noted elsewhere in the Agreement, including any Embedded Programs, Documentation, and Updates.
18. "**Software Subscription**" means Support Services for the term as provided in the Agreement and Fee Schedule.
19. "**Solution**" means the JMS Software and/or Cloud Hosted Environment provided by or supported by ATIMS and specifically listed in the Scope of Work (SOW) or Support Agreement.
20. "**Support Services**" – means the Cloud Hosting, Support, and Maintenance of the JMS, and any Additional Services, as defined herein.
21. "**Updates**" means "bug" fixes and other updates, enhancements, upgrades, new version releases, or re-releases of the Software which are made generally available without charge by ATIMS to ATIMS's Clients; provided, however, that Updates shall not include new applications for which ATIMS charges a fee to its Clients.
22. "**User**" means an individual, whether a County employee or contractor, to whom the County has created an account and password, to allow access to the JMS. ATIMS offers an unlimited number of users associated with user groups.
23. "**Workaround**" means a change in the procedures followed or data supplied by Client to avoid an Error without substantially impairing Client's use of the Solution.

2.0 Hosting Services

2.1 Term

ATIMS shall provide Support Services, including cloud hosting, maintenance and support services for the ATIMS's Jail Management System (JMS) application, referenced in the Agreement, and as set forth in the Support Agreement's Provisions, Use & Limitations for the term specified in Exhibit B: Payment and Fee Schedule.

Subject to the terms and conditions hereof, ATIMS hereby grants to the County a non-exclusive, non-transferable, annual subscription to access and use the Software, including any third-party Embedded Programs, users, employees, agents or contractors of the County as set forth in the Fee Schedule.

Except as otherwise provided herein or in the Agreement, County shall be liable for all acts and omissions of the Users.

2.2 Hosted Environment

ATIMS has sole responsibility for acquiring and maintaining a secured, Cloud Hosting Environment to host, for the County, the County's configured JMS software for the term of the subscription. ATIMS shall use the Amazon AWS gov cloud Platform. No change in the Cloud Hosting Environment can occur without formal notice of at least 90 days and agreement by the County.

In addition to all other representations and warranties set forth in the Agreement, ATIMS hereby represents and warrants to Client the following:

The Cloud Hosting Environment meets or exceeds the environment specifications required by the County, including performance metrics, as set forth in the Statement of Work and described herein. Prior to any installation and/or operation of the Software, ATIMS will ensure that the Cloud Hosted Environment is installed, configured, tested and prepared by ATIMS, and meets and/or exceeds the County's environment specifications. ATIMS shall be solely responsible for the supervision, management and operation of the Cloud Hosted Environment including without limitation:

1. Establishing County approved disaster recovery backup and failover plans, in the event of a hardware or Software failure or disaster
2. Implementing industry standard procedures to provide adequate security and accuracy of data
3. Security maintenance and password distribution as desired by the County

County represents and warrants to ATIMS that County will not make any material changes to the Cloud Hosted Environment, except solely as required and/or directed by ATIMS or as otherwise noted elsewhere in the Agreement.

2.3 Proprietary Rights/Confidentiality

ATIMS owns all right, title and interest (including but not limited to all copyrights, patents, trademarks, trade names, trade secrets and other proprietary rights) in, and to the Software and all components, reproductions, modifications or derivative works thereof, in whole or in part.

ATIMS may utilize all ideas, suggestions or feedback that Client provides to ATIMS with respect to the Software without any obligation to Client.

2.4 Business Use

County and its Users may use the Software subscription solely for official County operations. Any other use of the Software (including without limitation timesharing, rental, leasing, facility management, provision of subscription services or service bureau usage) is strictly prohibited.

2.5 No Rights to Code

The Subscription granted hereunder is for the object code version of the Software Subscription only. Other than otherwise set forth in a source code escrow agreement, County has no rights to the source code for the Software. County shall not and shall not permit anyone under County's direction or control, to reverse engineer, disassemble or de-compile the Software or attempt to do so. County may not modify, adapt, translate or create derivative works of the Software without ATIMS's express written consent. The Software is a single product. Embedded Programs may be used only in conjunction with the Software.

2.6 No Copies Allowed

County shall not copy the Software or any part thereof, however, the County may backup its data, without limitation, to either the Cloud Hosted Environment or a local environment.

2.7 Embedded / Third-Party Program (list)

As ATIMS is the Licensee of any Embedded Programs, ATIMS, not the County, shall be and remain subject to all terms, conditions and licenses imposed by the manufacturers and/or third- party licensors ("Licensors"), including ATIMS, of such Embedded Programs.

3.0 ATIMS Requirements & Responsibilities

3.1 Server Environment

ATIMS is providing a Software-as-a-Service (SaaS) hosted solution, and therefore all software and hardware components, including Embedded Programs needed for the ATIMS JMS to operate, and all software Updates will be provided to the County.

The ATIMS Cloud Hosted Environment includes the following components:

- **Web Server** using Amazon Linux 2 VM. The purpose of this web server is to deliver initial "compiled Angular application" to the browser.
- **Application Server**. This is the ASP.NET Core application. It is deployed on Windows 2019 or a later Windows operating system, SQL Server-based Database Server 2019 or later. This is deployed in the hosted (PAAS) mode on Amazon RDS.
- **Report Server**. ATIMS has licensed the JSReports framework that enables production of customers' build reports using only HTML and JavaScript skills. JSReport is NodeJS application that is deployed on AWS Linux 2.

To maintain performance levels and operational efficiencies, ATIMS may upgrade and/or otherwise modify the system environment, upon notification and in consultation with the County.

The Server Environment may also include, upon the County's authorization, load balancing, database clustering, and a replication database.

As part of ATIMS Cloud Hosting Services, ATIMS shall provide, at no additional cost to the County, infrastructure upgrades, including hardware, network, and software (e.g., operating system, database) such that the County's performance requirements (See the SOW performance metrics) continue to be met without interruption or degradation. Software upgrades shall not be more than one major release behind the current release available from the provider of the infrastructure component. Scheduling of software and hardware upgrades will be coordinated with the County and implemented upon County's approval.

3.2 Monitoring

ATIMS shall use a variety of tools to monitor performance and health of the JMS and Cloud Hosted Environment, including:

1) The availability and performance of County's production services environment.
2) The operation of infrastructure and network components.

ATIMS will use a number of metrics in AWS CloudWatch service to monitor CPU and memory utilization. Additionally, ATIMS will monitor API response time alerting ATIMS support staff in case users experience degradation, even if the system itself appears to be healthy. ATIMS will provide the County with access to the AWS CloudWatch dashboard and related AWS tools during the implementation and while providing Cloud Hosting Services.

ATIMS shall monitor all levels of the service infrastructure, and generate alerts for CPU, memory, storage, database, network components, and transactions. Performance testing and metrics specified in the Statement of Work during the implementation of the JMS will continue to be provided and met during the term of this Support Agreement.

ATIMS support staff will attend to any automated warnings and alerts associated with deviations of the environment from ATIMS and Client defined monitoring thresholds and will follow ATIMS standard operating procedures (SOPs) to investigate and resolve underlying issues.

3.3 Regulatory Compliance

ATIMS shall maintain continuous regulatory compliance as a standard part of ATIMS business practices. The ATIMS Architecture and Custody Operation teams will stay current using a number of sources, including, but not limited to NIST, CJIS, Cloud Security Alliance; Software Vendors Bulletins (SVE and MITRE's CWE); as well as Federal and State government guidelines.

The ATIMS JMS will provide CJIS access controls by way of physical location (workstations), and Network addresses. ATIMS staff are required to be trained, tested, and certified in CJIS security policies, including the CJIS Security Addendum

ATIMS, and any ATIMS subcontractors, will follow the latest FBI CJIS security and training requirements for all JMS clients and CLETS PPP for California clients at no additional cost to the County. Additionally, ATIMS will follow the Cloud Security Alliance Cloud Control matrix, encrypting in transit and at rest. ATIMS staff will be background-checked before hire, and as required by the County. ATIMS will provide CJIS annual training, or as specified by the latest CJIS policy, and limit access to customer data to staff that has a legitimate need. Per ATIMS, the JMS solution is a highly secure, CJIS compliant hosted solution with Amazon Web Services GovCloud region and ATIMS will provide the County with compliance reports on an agreed upon schedule per CJIS Policy 5.9.4 and on demand by the County.

ATIMS will work with the AWS Law & Justice Group to implement best practices and ATIMS will provide prompt remediation of any identified compliance issues.

3.4 Audit and Security Requirements

ATIMS will provide a highly secure, CJIS compliant hosted solution with Amazon Web Services GovCloud region. As part of the Hosting services, ATIMS is responsible for vulnerability scanning and security. ATIMS will provide the County with copies of security scanning and audit reports quarterly, and the AWS SOC Type 2 report annually, for the client environment where the County’s application is hosted. The County will be

notified promptly of any issues found during regular security scanning and auditing. ATIMS will be responsible for remediation and notice to the County of the results.

3.5 Backup and Disaster Recovery

ATIMS shall advise and coordinate with the County on creating backup and disaster recovery policies and practices.

3.6 Failover

The JMS will operate in a 24/7/365 high-volume environment. In the event of a partial or total failure of the primary hosting site, the JMS system will be able to operate using geographically distributed and load balanced or clustered application nodes or have complete fail-over capability -- including all interfaces -- to an alternate hosting location. All locations where the application is hosted at will meet all applicable County and FBI CJIS security requirements. In addition, the system will be engineered and implemented to County standards such that loss of access and data is minimized in the event of system, cloud data center, network, or other types of failure.

4.0 County Requirements & Responsibilities

4.1 Access to County Resources

County shall provide ATIMS with reasonable access to County's technical personnel, facilities, systems, databases, and information for ATIMS to perform its obligations under this Agreement, subject to County's security and safety rules.

4.2 Appointment of Agency Manager and Contacts

County shall appoint a point of contact to act as liaison between the County and ATIMS.

To optimize the process of providing services and support, Sonoma County Sheriff′s Office will designate Technical Services Bureau Staff as authorized Agency Support Contacts able to submit Support Services requests to ATIMS, of whom one will be designated a **primary contact** and one an **alternate contact.** The primary and alternate contacts will have final authority on requests and decisions.

4.3 Assistance

County shall provide reasonable information and assistance to ATIMS to enable ATIMS to implement the ATIMS JMS solution and provide Cloud Hosting Services. Client acknowledges that ATIMS ability to implement and deliver the Cloud Hosting JMS Solution and Services in the manner provided in this Agreement may depend upon the accuracy and timeliness of such information and assistance.

4.4 Compliance with Laws

County shall comply with all applicable laws and regulations.

4.5 Unauthorized Use; False Information

County shall:

1) Notify ATIMS promptly of any unauthorized access to JMS and shall use reasonable efforts to terminate such unauthorized access.
2) Not provide false identity information to gain access to or use the JMS and Cloud Hosting Services.

4.6 Administrator Access

County shall be solely responsible for the acts and omissions of its Administrator Users.

4.7 Client Content

County is solely responsible for collecting, inputting and updating all Client Content stored on the JMS Cloud Hosting Environment, and for ensuring that the Client Content does not contain anything that is obscene, defamatory, harassing, offensive or malicious.

4.8 License from Client

Subject to the terms and conditions of this Agreement, County shall grant ATIMS a limited, non-exclusive and non-transferable license, to copy, store, configure, display and transmit Client Content solely as necessary to provide the JMS Cloud Hosting Services to Client Agency.

4.9 Ownership & Restrictions

The County retains ownership and intellectual property rights in and to all County Data. ATIMS or its licensors retain all ownership to the jail management system. Third-party technology that may be appropriate or necessary for use with some ATIMS programs, and the County's s right to use such third -party technology is governed by the terms of the third-party technology license agreement between the third party and ATIMS.

4.10 Suggestions

ATIMS shall have a royalty-free, , irrevocable, perpetual license to use and incorporate into the JMS any County suggestions for JMS product improvements.

4.11 Software Installation

Upon installation of any Software or Hardware upgrades to the JMS or Cloud Hosted Environment, County agrees to follow reasonable release installation instructions, review system operations after installation, and report any Issue detected as soon as possible.

4.12 Key Encryption

The County will upload key material from an on-premise key store and transmit the encrypted key to AWS, which will become the Customer Managed Key (CMK). County will own the key but provide access to ATIMS for use with AWS.

5.0 Support & Maintenance Services

5.1 Overview

This Support Agreement includes Cloud Hosting, Support, and Maintenance Services including:

Cloud Hosted Environment and Services, including:

- Development and maintenance, including software and hardware components, of a minimum of five environments (Production, Test, Training, Development, Reporting) during the Support Agreement term
- Periodic health checks of the production system, and notification to the County of performance issues and any unauthorized access
- Ongoing tuning and other required system level administration
- Recommendations for upgrades to the Cloud Hosted Environment to better accommodate the JMS

Support of the JMS, including:

- Level 2 help desk support, including:
  1. Monitoring and responding to discovered system issues
  2. Corrections and Fixes, including code corrections, to resolve Solution malfunctions in order to bring such Solution into conformity with the operating specifications, Documentation, and Statement of Work
- Telephone and electronic support to fix issues reported by the County to ATIMS
- Up to seven (7) Agency Support Contacts designated by County with authority to directly contact ATIMS and report issues

Maintenance of the JMS, including:

- JMS Updates (e.g., Upgrades)
- Updates and maintenance of an electronic copy of Documentation accessible online via the JMS
- Impact analysis of upcoming patches and Updates
- Modifications to ATIMS provided components and configurations to support upcoming patches and Updates
- Testing and deployment of Updates and patches and in all County environments
- Application modifications required to support scheduled Could Hosted Environment infrastructure upgrades and changes

- Service Credits in the form of an allocation of County's support fees to be allocated to Professional Services (See Section 5.8 Service Credits)

5.2 Agency Tier 1 Support

The Client Agency will identify System Administrators or other individuals to provide Tier 1 JMS support and troubleshooting. County support resources shall serve as the first point of contact with County end users and will initiate troubleshooting in coordination with other County resources as needed.

The purpose of Tier 1 support is to determine if the issue is a County issue (e.g., internal infrastructure, training, configuration, or permissions), to be resolved by the County, or if the issue needs to be reported to ATIMS support.

5.3 ATIMS Support Availability

Emergency Support
ATIMS understands that the County works 24/7/365 and in addition to support during standard business hours, ATIMS provides 24/7/365 emergency support, to meet those requirements.

Standard Support
Standard Business hours 0800--1700 PST, Monday thru Friday, except holidays, are used for response to non-emergency requests.

5.4 ATIMS Contact Methods

ATIMS provides several methods for the County to contact ATIMS to report an issue and engage ATIMS Level 2 Support

- **Email** – Support via email is provided at Support@ATIMS.com.
- **Telephone** – Support via telephone is provided 24/7 365 at 833.291.4428.
- **JIRA -** An online support tool which the County can use to report an issue by creating a ticket.

JIRA is used by ATIMS to track all releases, upgrades, defects and regularly and ad hoc maintenance calls. As a standard course of action, ATIMS support staff will also use JIRA to track all details and disposition of a support request including caller information, any current corrective action taken, any future activity required and final status. The Agency's Point of Contact(s) will have access to JIRA, including the ability to view all records/tickets.

The County will report issues via JIRA, using email if JIRA is not available, and Telephone when an issue is Critical.

5.5 ATIMS Remote Diagnostics

ATIMS typically uses two platforms (Zoom and Teams) to provide remote diagnostics and support. ATIMS performs online diagnostics from ATIMS's offices to assist in the identification and isolation of suspected Software or Solution errors or malfunctions.

In the event the County requires the use of another remote diagnostic tool or service, the County must provide access to the required tool at no cost to ATIMS. ATIMS will make best efforts to comply with the security requirements of the Client. Any Security configuration(s) needed to achieve remote connectivity and/or access to County' s computer network will be used only for the purposes of diagnosing the "error" or malfunction.

5.6 ATIMS Engagement Process

ATIMS will provide support to the County through the following process:

- **Initial Engagement** – An Agency Support Contact will contact ATIMS through one of the support methods to place a request for service.
- **Discovery** - ATIMS Support Desk will gather all of the necessary information from the County to assess the situation. The support technician will determine the appropriate course of action such as ask the County to attempt various tasks or begin a remote session via an online connection. This Discovery Period will be completed in 30 minutes or If a resolution has not been achieved at the end of the Discovery Period, then the support technician will open a ticket for further investigation of the issue.
- **Professional Service** - If the engagement is deemed to require Professional Services outside of the scope of Support & Maintenance, the County POC will be given an estimated cost to complete the requirement at a $200/hour blended labor rate.
- **Updates** - Client Agency will be updated on a regular basis on the status of an issue and will be provided resolution logs when a support ticket is successfully closed. (See Section 6. Service Level Agreement)
- **Resolution** - ATIMS will make best efforts to resolve the issue as quickly as possible. Please note that additional remote sessions via an online connection may be required during this period.

5.7 Upgrades

ATIMS will provide to County at no additional cost all Upgrades. County will determine whether to accept an Upgrade and when it will be implemented.

All customizations/enhancements (e.g., modified or new functionality/modules, reports, integrations, tools) created for other customers will be made available at no additional charge as a configurable option for the County to use.

Upgrades will be accompanied by comprehensive release notes and appropriate documentation, including user guides with screenshots and detailed explanations of changes, Jira lists of included tickets, video recording

walkthroughs, and updated technical documentation (e.g., data dictionary, ERD) to allow JMS administrators and end users to understand, configure, and effectively use any new or modified functionality.

ATIMS will provide to the County each quarter their current roadmap and planned release schedule of system functionality.

5.8 Service Credits

ATIMS's annual Cloud Hosting Support & Maintenance includes an allotted number of hours (value) towards the County's needs each year. These hours can be used towards any type of professional service including, enhancements, training, and customized form, report and interface development.

The value of these hours is included in the annual recurring fees and, unless changed via a change/order or contract amendment, is $40,000 at the previously noted $200/hour rate

Hours are added each year at the contract anniversary. Unused hours will rollover to the next contract year. An itemized accounting of used and remaining hours will be provided upon County request or at the end of each contract year.

6.0 Service Level Agreement (SLA)

6.1 Support - ATIMS Tier 2 Response & Resolution Times

ATIMS shall provide Tier 2 Support to the County for issues reported by Agency Support Contacts.

Priority & Communications - When reporting an Incident, the County will make the initial determination of priority and include it in the request. ATIMS's initial response to an incident will be based on the Agency's assessment of priority. ATIMS will make best efforts to respond to support requests within the timeframes outlined below. Periodic status updates will be provided via email and phone until the issue is satisfactorily resolved; status can also be checked online via ATIMS JIRA support site.

After the initial response, any changes to the incident priority will be mutually determined by ATIMS and the County.

Priority Levels & Response ATIMS JMS Service Levels will be determined using the following priority table; and Support will be provided in accordance with the Service Level for that issue:

PRIORITY and Severity Levels	CRITICAL - 1	HIGH 2	MODERATE - 3	LOW - 4
Description	• System down • Critical issues with, or inability to perform core functions or critical processes of JMS • Security breaches and other security issues • Business risk is Critical.	• Software Application Program errors without application workarounds • Incorrect calculation errors impacting records • Severe performance issues impacting critical processes • Business risk is High	• System errors that have workarounds • Performance issues not impacting critical processes • Usability issues • Reporting Issues • Business risk is moderate	• Report formatting • Aesthetic issues • Recommendations for enhancements on system changes • Low to minimal impact
Response Time	< 30 minutes	1 hour	2 hours	8 hours
Update Frequency	Every 30 min	Every 2 hours	Every 24 hours	Every 10 business days
Resolution Goal	Within 30 minutes.	Within 2 hours.	Within 5 business days	Within 30 business days. Placed in queue and resolved in order of importance

Description Examples.

Critical

- Major system failure: no users can login or use the application at all.
- The system crashes or freezes completely when a particular action is executed.
- Inability to perform a critical task, including intake, classify, house, move, release an inmate

High

- A mandatory field in a record will not allow entry of data into it and therefore the record as a whole cannot be saved. There is no work around.
- System performance is significantly degraded, requiring excessive time to complete an operation.

Moderate

- A date field does not default the current date as detailed in the design, but the user can manually go and select a date.
- Scheduled report does not email automatically as configured; however, report can be manually run by user and sent via email as attachment.

Low

- Spelling mistake on a field label.
- Spacing between columns is irregular.
- Wrong date format.

Response Definitions

- **Response Time**: the maximum elapsed time after a problem is reported to ATIMS Support that ATIMS acknowledges the Issue, assigns the Issue to ATIMS personnel, and provides a date/ time assigned and a severity level to the County. ATIMS will communicate with the Agency's internal software support team and provide an action plan.
- **Update Frequency**: the maximum time elapsed after problem has been initially reported before a status update is provided to the Agency. ATIMS will continue to provide status updates to the Agency within this frequency interval until the problem is resolved.
- **Resolution Goal**: the objective for the maximum elapsed time after a problem is reported for resolution of the problem is provided.

Related Definitions :

- "Correction/Fix" means the repair or replacement of Software component(s) to remedy an Issue.
- "Issue" means a defect in Software as defined in ATIMS's standard Software specification that significantly degrades such Software.
- "Workaround" means a change in the procedures followed or data supplied by Client to avoid an Issue without substantially impairing Client's use of the Software.

ATIMS will use best efforts to provide a problem resolution within the stated Service Resolution time goal.

In the event that ATIMS receives a surplus of PSS requests simultaneously, clients will be prioritized by Severity Level and in the order the incidents are reported.

6.2 Support - Onsite Option

Remote diagnostics will be the first course of action to resolve an incident or technical assistance prior to an onsite visit being scheduled.

Onsite support, unless otherwise agreed, will be provided during regular Business Days and Hours, 0800 – 1700 Pacific Standard Time, Monday through Friday, excluding ATIMS holidays. ATIMS's Holiday Schedule will be provided.

If a problem occurs which significantly impacts the Client's usage of the licensed product and the issue remains unidentified or unresolved either by workaround or permanent correction after the Client has followed ATIMS prescribed actions, ATIMS may provide, or ATIMS and the Client may agree, to onsite support.

Once dispatched, the support technician will arrive at the agreed upon time and keep the County fully informed during the period onsite. PSS for onsite visits that require air travel will be arranged on a case-by-case basis and the travel cost will be confirmed with the County prior to booking.

ATIMS will provide or make available:

1) Assistance in diagnosis and identification of errors or malfunctions.
2) Onsite consultation on correction of identified errors or malfunctions.
3) Detailed feedback on external factors that had a direct or indirect impact on the software resulting in performance deficiencies.

Travel Expense - Onsite support performed by ATIMS employees for a Client Agency requires Client approval for payment of travel and/or living expenses incurred by ATIMS. For Client-initiated tasks, actual expenses will be billed at cost, *as* they are incurred. County may choose to use Service Credits defined in Section 5.8 toward Travel Expenses.

6.3 Hosting - Service Guarantee

ATIMS will provide 99.9% availability on a 24/7 basis outside of scheduled maintenance windows.

Availability (for 99.9%) would be calculated as follows:

((Total – Non excluded – Excluded)/(Total-excluded))*100 >99.9% Description of calculations:

1. Total means the total number of minutes in the calendar quarter.
2. Non-excluded means downtime that is not excluded; and
3. Excluded means:
   a) Any planned downtime of which ATIMS gives 24 or more hours' notice in accordance with the Agreement.
   b) Any unavailability caused by circumstances beyond ATIMS reasonable control, including,

without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving ATIMS employees), denial-of-service attacks, or third-party Internet service provider failures/delays at Client Agency.

c) Any unavailability that is caused by system components outside ATIMS control, such as enterprise authentication or third-party interfaces

6.4 Hosting - Recovery Point Objective

The solution RPO (Recovery Point Objective) data loss threshold is fifteen (15) minutes.

6.5 Hosting - Recovery Time Objective

The solution RTO (Recovery Time Objective – tolerance to service interruptions) is thirty (30) minutes.

ATIMS shall advise and coordinate with the County on procedures and infrastructure to maintain Business Continuity during and after system failure.

6.6 Remedies

ATIMS and County shall negotiate in good faith remedies for degraded performance, system issues, system failure, and other failures, for example, resolution times repeatedly or significantly in excess of the service level goal. An example of a remedy would be a credit that can be applied for services (e.g., reports, forms, development work, training, fees owed).

7.0 Professional Services & Support (PSS)

7.1 Optional Professional Services

ATIMS provides Professional Services and Support (PPS) to give client s the opportunity to acquire services beyond the scope of the Support Agreement. Professional Services are provided at a $165 /hour blended rate.

Examples of services that are available at the option of the County include:

- Enhancement (customization) of ATIMS JMS
- Business Process Re-engineering
- Workflow Development or Redevelopment
- New or Updated Interfaces or Integrations
- Additional Training
- Hardware Procurement or Installation

7.2 Support Discovery

In response to a Support ticket, once Discovery with the Client POC and ATIMS Support Desk is completed, if the engagement is deemed beyond the scope of the Cloud Hosting agreement and rather part of Professional Services (see above), the Client Agency POC will be given an estimated cost to complete the requirement.

7.3 Fees

County will be billed in hourly increments, based on rates provided in the Payment and Fee Schedule, for all Professional services or time will be charged against annual allotment of hours (as part of annual Support Agreement). Where the County requests onsite support, there will be a minimum two-hour charge for onsite support, not including travel time. All PSS hours will be tracked by the assigned technician and verified by the ATIMS Support Manager. County will be updated on a regular basis on the status of the Request (or issue) and will be provided resolution logs when a support ticket is successfully closed or work is completed.

8.0 Terms and Conditions

8.1 Limitations of Liability

Except in the case of gross negligence or willful misconduct in no event shall either party be liable to the other for incidental, indirect, special or consequential damages of any kind, however caused and on any theory of liability arising out of or in connection with the services or program or solution provided pursuant to this Agreement.

8.2 Use of County JMS and Computer Systems

When ATIMS performs services pursuant to this Agreement which require the use of the County's computer system(s), the County agrees to make it available at reasonable times and time increments, at no charge to ATIMS.

County agrees to furnish ATIMS access to the JMS when performing service, subject to County's reasonable industrial security and safety rules. County must support remote problem diagnosis and maintenance.

Exhibit M
Technical Requirements

Confidential

Exhibit N
Functional Requirements

Confidential

Exhibit O
Interfaces and Data Exchanges

Confidential